INSO
16343-1
1st.Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
۱۶۳۴۳-۱
چاپ اول
۱۳۹۴

مهندسی سامانه‌ها و نرم‌افزار – تضمین سامانه‌ها و نرم‌افزار – قسمت ۱: مفاهیم و واژگان

Systems and software engineering — Systems and software assurance — Part1: Concepts and vocabulary

ICS: 35.080

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« مهندسی سامانه‌ها و نرم‌افزار – تضمین سامانه‌ها و نرم‌افزار - قسمت ۱: مفاهیم و واژگان »

رئیس:	**سمت و/ یا نمایندگی:**
دانند‌ه، آزاده (کارشناسی مهندسی کامپیوتر)	مدیرعامل شرکت فناوران اطلاعات بهاران
دبیر:	
فرهاد شیخ احمد، لیلا (کارشناسی‌ارشد مهندسی کامپیوتر - نرم‌افزار)	کارشناس استاندارد سازمان ملی استاندارد ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
آذرکار، علی (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	مدیرعامل شرکت پدیدپرداز، عضو هیأت مدیره سازمان نظام صنفی رایانه کشور
بی‌مانند، هدی (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	کارشناس رایانه و فناوری اطلاعات اداره استاندارد استان ایلام
جمشید عینی، مریم (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	مدیر شبکه و رئیس سیستم شبکه مجتمع قضایی خانواده شماره یک
سجادی، ندا (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	کارشناس ارشد بانک پارسیان
سعیدی، عذرا (کارشناسی‌ارشد مهندسی مخابرات)	کارشناس استاندارد سازمان فناوری اطلاعات ایران
شیرازی میگون، مریم (کارشناسی مهندسی فناوری اطلاعات)	کارشناس پژوهشگاه سازمان ملی استاندارد ایران
قسمتی، سیمین (کارشناسی‌ارشد مهندسی فناوری اطلاعات)	کارشناس استاندارد سازمان فناوری اطلاعات ایران – مشاور مرکز اپای دانشگاه تربیت مدرس
معروف، سینا (کارشناسی مهندسی کامپیوتر، سخت‌افزار)	کارشناس شبکه – کارشناس سازمان فناوری اطلاعات ایران
نشاط میبنی تهرانی. مهنوش (کارشناسی‌ارشد مترجمی زبان انگلیسی)	پژوهشگر گروه واژه‌گزینی فرهنگستان زبان و ادب فارسی

ویراستار:

قسمتی، سیمین
(کارشناسی‌ارشد مهندسی فناوری اطلاعات)
کارشناس استاندارد سازمان فناوری اطلاعات ایران – مشاور
مرکز اپای دانشگاه تربیت مدرس

فهرست مندرجات

عنوان **صفحه**

آشنایی با سازمان ملی استاندارد ایران ..... ج
کمیسیون فنی تدوین استاندارد ..... د
پیش‌گفتار ..... ح
مقدمه ..... ط
۱ هدف و دامنه کاربرد ۱
۲ کاربست‌پذیری ۱
۲-۱ مخاطبان ۱
۲-۲ حوزه کاربست ۲
۳ اصطلاحات و تعاریف ۲
۳-۱ اصطلاحات مرتبط با تضمین و خواص ۲
۳-۲ اصطلاحات مرتبط با محصول و فرایند ۴
۳-۳ اصطلاحات مرتبط با سطح یکپارچگی ۵
۳-۴ اصطلاحات مرتبط با شرایط و پیامدها ۶
۳-۵ اصطلاحات مرتبط با سازمان ۸
۴ ساختار این استاندارد ۹
۵ مفاهیم پایه ۱۰
۵-۱ مقدمه ۱۰
۵-۲ تضمین ۱۰
۵-۳ سودبران ۱۱
۵-۴ سامانه و محصول ۱۱
۵-۵ خاصیت ۱۱
۵-۵-۱ خواص به‌عنوان رفتار ۱۲
۵-۶ عدم قطعیت و وثوق ۱۳
۵-۷ شرایط و رویدادهای آغازین ۱۳
۵-۸ پیامدها ۱۴
۶ استفاده از قسمت‌های چندگانه این مجموعه استاندارد ۱۵
۶-۱ مقدمه ۱۵
۶-۲ راهنمای کاربرد ابتدایی ۱۵
۶-۳ ارتباطات میان قسمت‌های این مجموعه استاندارد ۱۶

۶-۴ مراجع ۱۷
۷ این مجموعه استاندارد و مورد تضمین ۱۷
۷-۱ مقدمه ۱۷
۷-۲ توجیه روش برهان ۱۹
۷-۳ ابزار دست‌یابی به شاهد و مدیریت شواهد آن ۲۰
۷-۴ صدور گواهی و اعتباردهی ۲۰
۸ این مجموعه استاندارد و سطوح یکپارچگی ۲۱
۸-۱ مقدمه ۲۱
۸-۲ تحلیل مخاطره ۲۲
۹ این مجموعه استاندارد و چرخه عمر ۲۳
۹-۱ مقدمه ۲۳
۹-۲ فعالیت‌های تضمین در چرخه عمر ۲۴
۱۰ خلاصه ۲۵
کتاب‌نامه ۲۶

پیش‌گفتار

استاندارد « مهندسی سامانه‌ها و نرم‌افزار – تضمین سامانه‌ها و نرم‌افزار - قسمت ۱: مفاهیم و واژگان » که پیش‌نویس آن در کمیسیون‌های مربوط تهیه و تدوین شده است، در چهارصد و نوزدهمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۴/۱۲/۲۴ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی (منابع و مآخذی) که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 15026-1:2013, Systems and software engineering — Systems and software assurance —Part1: Concepts and vocabulary

مقدمه

این استاندارد یکی از استانداردهای مجموعه استاندارد ملی ایران به شماره۱۶۳۴۳ است. تضمین نرم‌افزار و سامانه‌ها و فیلدهای مرتبط نزدیک با آن، مفاهیم مشترکی دارند ولی دارای واژگان مختلف و نقطه نظرات متفاوتی هستند. این استاندارد ملی، مجموعه واحدی از مفاهیم اصلی و استفاده بدون ابهام از مجموعه اصطلاحات در میان این فیلدهای مختلف ارائه می‌کند. این استاندارد، مبنایی برای همکاری، مباحثه، توافقات ثبت شده و منطق عطف به مفاهیم و واژگان به‌کاررفته به طور یکسان درمیان این مجموعه استاندارد ارائه می‌کند.

این استاندارد، مفاهیم موردنیاز برای درک تضمین نرم‌افزار و سامانه‌ها و به طور خاص، آن مفاهیم اصلی به منظور استفاده از قسمت دوم و چهارم این مجموعه استاندارد را روشن می‌کند. این استاندارد از مفاهیم مشترک، موضوعات و اصطلاحات کاربردپذیر در میان گستره خواص، دامنه‌های کاربرد و فناوری‌ها پشتیبانی می‌کند.

مهندسی سامانه‌ها و نرم‌افزار– تضمین[1] سامانه و نرم‌افزار– قسمت ۱: مفاهیم و واژگان

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و تعریف اصطلاحات مرتبط با تضمین است و مجموعه‌ای سازمان‌یافته از مفاهیم و ارتباطات را تعیین می‌کند تا مبنایی برای درک مشترک درمیان جوامع کاربران برای تضمین، ایجاد شود. این استاندارد، اطلاعاتی را به کاربران دیگر قسمت‌های این مجموعه استاندارد از جمله کاربرانی که از کل این مجموعه استاندارد استفاده می‌کنند، ارائه می‌کند. مفهوم اصلی معرفی شده توسط این مجموعه استاندارد، بیان *ادعا*[2] برای یک *مورد تضمین* و پشتیبانی از آن ادعاها از طریق *استدلال*[3] و *شواهد*[4] است. این ادعاها، در زمینه تضمین خواص سامانه‌ها و نرم‌افزار درون فرایندهای چرخه حیات سامانه یا محصول نرم‌افزاری است.

تضمین خدمتی که در یک روال جاری، در حال بهره‌برداری و مدیریت است، در این استاندارد پوشش داده نمی‌شود.

۲ کاربست‌پذیری[5]

۲-۱ مخاطبان

کاربران بالقوه این مجموعه استاندارد متنوع هستند از جمله توسعه‌دهندگان و نگاهدارندگان موارد تضمین و آن کسانی که خواهان توسعه، ابقاء، ارزشیابی یا اکتساب سامانه‌ای هستند که این نیازمندی‌ها را برای خواصِ مشخص به طریقی تحمیل می‌کنند تا از آن خواص و نیازمندی‌های خود قطعیت بیشتری پیدا کنند. این مجموعه استاندارد از مفاهیم و اصطلاحات سازگار با استانداردهای ISO/IEC 12207 و ISO/IEC 15288 استفاده می‌کند و عموماً با مجموعه استانداردهای خانواده ISO/IEC 25000 سازگار است ولی کاربران بالقوه استاندارد ISO/IEC 15206 نیاز به درک تفاوت‌ها از مفاهیم و اصطلاحاتی دارند که ممکن است با آن آشنایی داشته باشند. این استاندارد ملی تلاش به روشن‌سازی این تفاوت‌ها دارد.

1 - assurance
2 - claim
3 - argumentation
4 - evidence
5 - applicability

۲-۲ حوزه کاربست

قصد اولیه این استاندارد ملی، کمک به کاربران دیگر قسمت‌های این مجموعه استاندارد از طریق ارائه زمینه، مفاهیم و توضیحات برای تضمین، موارد تضمین و سطوح یکپارچگی است. جزییات مربوط به چگونگی سنجش، مصورسازی یا تحلیل خواصِ مشخص، با وجودی که برای امور اجرایی ضروری است، پوشش داده نمی‌شود.. این موارد، موضوعات استانداردهای بسیار خاصی هستند که به تعدادی از آنها ارجاع داده شده و در کتاب‌نامه گنجانده شده‌اند.

مراجع الزامی[1]

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات با تعاریف زیر به کار می‌رود:

یادآوری- این اصطلاحات به منظور یکسان‌سازی در سراسر این مجموعه استاندارد در نظر گرفته شده است.

۳-۱ اصطلاحات مرتبط با تضمین و خواص

۳-۱-۱

تضمین

assurance

مبنایی برای وثوق سنجیده[2] به این که یک ادعا انجام شده یا می‌شود.

۳-۱-۲

ادعا

claim

بیانیه‌ای با خصلت صحیح/غلط در مورد حدودِ مقادیرِ خاصیتی که بدون ابهام تعریف‌شده، که خاصیت مورد ادعا نامیده می‌شود، و حدود مرتبط با عدم قطعیت مقادیر خاصیت مرتبط با حدود ذکر شده که حدود اولیه است، طی زمان مطرح بودن ادعا و تحت شرایط مشخص موضوع ادعا.

یادآوری ۱ مدخل- همچنین عدم‌قطعیت‌ها ممکن است با مدت زمان کاربست و شرایط بیان شده مرتبط باشند.

یادآوری ۲ مدخل- یک ادعا، به طور بالقوه، شامل موارد زیر است:

۱- این استاندارد دارای مراجع الزامی نیست.

2 - justified confidence

- خاصیت ادعا
- محدودیت مقدار خاصیت مرتبط با ادعا (به طور مثال: در مورد گستره آن)
- محدودیت در مورد عدم‌قطعیت مقدار خاصیتی که محدودیت آن را برآورده می‌سازد
- محدودیت در مورد مدت زمان کاربست‌پذیری ادعا
- عدم‌قطعیت مرتبط با مدت زمان
- محدودیت در مورد شرایط مرتبط با ادعا
- عدم‌قطعیت مرتبط با شرایط

یادآوری ۳ مدخل- اصطلاح «محدودیت» به منظور متناسب‌سازی وضعیت‌هایی که می‌تواند موجود باشد، به کار می‌رود. مقادیر می‌تواند مقدار واحد یا چندین مقدار واحد یا گستره‌ای از مقادیر یا چندین گستره از مقادیر باشد و همچنین می‌تواند چند بُعدی باشد. کرانه این حدود برخی اوقات دقیق نیست، به طور مثال، ممکن است به طور احتمالی توزیعی بوده و یا به صورت افزایشی باشند.

۳-۱-۳

مورد تضمین

assurance case

فرآورده مستدل و قابل‌ممیزی ایجاد شده که از بحث درمورد مرتفع‌سازی ادعای سطح بالای آن (یا مجموعه ادعاها) پشتیبانی می‌کند، از جمله استدلال‌های نظام‌مند و شواهد اصلی آنها و مفروضات صریح که از ادعا(ها) پشتیبانی می‌کنند.

یادآوری ۱ مدخل- یک مورد تضمین شامل موارد زیر و ارتباطات آنها است:

- یک یا چند ادعا درمورد خواص
- استدلال‌هایی که به طور منطقی شواهد و هرگونه فرضی را به ادعا(ها) پیوند می‌دهد.
- مجموعه شواهد و مفروضات محتمل که از این استدلال‌ها برای ادعا(ها) پشتیبانی می‌کند
- توجیه انتخاب ادعای سطح بالا و روش استدلال

۴-۱-۳

اتکاپذیری

dependability

اصطلاح عمومی که به منظور توصیف عملکرد دسترسی‌پذیری و عوامل تأثیرگذار آن: عملکرد اطمینان‌پذیری، عملکرد نگهداشت‌پذیری و عملکرد پشتیبانی نگهداشت، به کار می‌رود.

یادآوری ۱ مدخل- اتکاپذیری تنها بری توصیف‌های عام در اصطلاحات غیرکمی به کار می‌رود.

یادآوری ۲ مدخل- استاندارد ISO/IEC 25010 بیان می‌کند که «خصیصه‌های اتکاپذیری شامل دسترسی‌پذیری و عوامل تأثیرگذار موروثی یا خارجی از قبیل اطمینان‌پذیری، تحمل خطا، قابلیت پوشش‌دهی مجدد، یکپارچگی، امنیت،

نگهداشت‌پذیری، قابلیت دوام و پشتیبانی نگهداشت است». بیشتر استانداردها اتکاپذیری را نشان می‌دهند (به طور مثال، [۶۴] و [۶۹]) و بیشتر از این کیفیت‌های داخل آن را نشان می‌دهند. استاندارد IEC 60050-19 تعاریف مرتبط را پیشنهاد می‌دهد.

[منبع :IEC 60300-1:2003]

۳-۲ اصطلاحات مرتبط با محصول و فرایند

۳-۲-۱

فرایند

process

مجموعه فعالیت‌های وابسته به هم یا متعامل است که ورودی‌های را به خروجی‌ها تبدیل می‌کند.

[منبع: ISO/IEC 15288:2008 و ISO/IEC 12207:2008]

۳-۲-۲

دید فرایند

process view

توصیفی از چگونگی دست یافتن به مقاصد مشخص شده و مجموعه دستاوردها از طریق به کارگیری فعالیت‌ها و کارهای فرایندهای موجود است.

[منبع: زیربند ت-۳، استاندارد ISO/IEC 15288:2008]

۳-۲-۳

محصول

product

نتیجه یک فرایند است.

یادآوری ۱ مدخل- نتایج می‌تواند عناصر، سامانه‌ها، نرم‌افزار، خدمات، قواعد[1]، مستندات یا اقلام بی‌شمار دیگری باشد.

یادآوری ۲ مدخل- «نتیجه» می‌تواند در برخی موارد تعدادی نتیجه منفرد مرتبطی باشد. اگرچه معمولاً ادعاها به نسخه‌های مشخصِ محصول مرتبط می‌شود.

[منبع: ISO/IEC 15288:2008 و ISO/IEC 9000:2005]

1 - rules

۴-۲-۳

سامانه

system

ترکیبی از عناصر متعامل سازمان‌یافته به منظور دست‌یابی به یک یا چند مقصود بیان شده است.

یادآوری ۱ مدخل- سامانه ممکن است به عنوان محصول یا خدماتی که ارائه می‌کند در نظر گرفته شود.

یادآوری ۲ مدخل- در عمل، ترجمهٔ معنی آن، به صورت تکرارشونده با استفاده از یک اسم تداعی‌کننده به طور مثال، سامانه هواپیمایی روشن می‌شود. متناوباً کلمه «سامانه» ممکن است به سادگی با یک مترادف وابسته به متن به طور مثال، هواپیما ولو این که ممکن است چشم‌انداز اصول سامانه را در خود مستتر کند، جایگزین شود.

[منبع: ISO/IEC 15288:2008]

۵-۲-۳

نیازمندی

requirement

اظهاری که یک نیاز و محدودیت‌ها و شرایط مرتبط با آن را ترجمه یا بیان می‌کند.

یادآوری ۱ مدخل- نیازمندی‌ها در لایه‌های مختلفی وجود دارند و نیاز را به شکل سطح بالایی (به طور مثال، نیازمندی عناصر نرم‌افزاری) بیان می‌کنند.

[منبع: ISO/IEC 15288:2008]

۶-۲-۳

جزء سامانه

system element

عضوی از مجموعه عناصری که سامانه را تشکیل می‌دهند.

یادآوری ۱ مدخل- جزء سامانه، قسمت گسسته‌ای از سامانه است که می‌تواند به منظور به انجام رسانیدن نیازمندی‌های خاص، پیاده‌سازی شود. جزء سامانه می‌تواند، سخت‌افزار، نرم‌افزار، داده‌ها، انسان‌ها، فرایندها (به طور مثال فرایندهایی برای ارائه خدمت به کاربران)، رویه‌ها (به طور مثال، دستورات متصدی)، تسهیلات، موارد اطلاعاتی و موجودیت‌های طبیعی (به طور مثال، آب، موجودات زنده، مواد معدنی) یا هر ترکیب دیگری باشد.

۳-۳ اصطلاحات مرتبط با سطح یکپارچگی

۱-۳-۳

سطح یکپارچگی

integrity level

ادعای سامانه، محصول یا عنصر که شامل حدودی بر مقادیر خاصیت، دامنهٔ ادعای کاربست‌پذیری و عدم‌قطعیت مُجاز در خصوص دست‌یابی به ادعا است.

یادآوری ۱ مدخل- عموماً مقصود آن این است که نگهداری از حدود بر مقادیرِ خاصیتِ مرتبط با اقلام مربوطه، منجر به نگهداری مخاطرات سامانه داخل حدود شود.

یادآوری ۲ مدخل- پذیرش شده از استاندارد ISO/IEC 15026:1998

۲-۳-۳

نیازمندی‌های سطح یکپارچگی

integrity level requirements

مجموعه نیازمندی‌های مشخص شده تحمیلی بر جنبه‌های مرتبط با سامانه، محصول یا عنصر و فعالیت‌های مرتبط است تا دست‌یابی از سطح یکپارچگی تخصیص‌یافته به این معنی که، ادعا را مرتفع می‌سازد)، داخل حدود موردنیاز درعدم‌قطعیت نشان دهد؛ این امر شامل شواهدی است که باید بدان دست یافت.

یادآوری ۱ مدخل- از این رو که سطح یکپارچگی به عنوان یک ادعا تعریف می‌شود، دو عبارت «دست‌یابی از سطح یکپارچگی تخصیص‌یافته» و «مرتفع ساختن ادعای آن» هم‌ارز هستند.

یادآوری ۲ مدخل- در زیربندهای ۳-۳-۱ و ۳-۳-۲ در استاندارد ISO/IEC 15026:1998 متناوباً به هر دوی «سطح یکپارچگی» و «نیازمندی‌های یکپارچگی» ارجاع می‌شود. دومی به «نیازمندی‌های سطح یکپارچگی» تغییر یافته است و هردو برای افزایش وضوح است چرا که این موضوع کاربرد رایجی در ایمنی دارد.

یادآوری ۳ مدخل- استاندارد IEEE Std 1012:2004، «سطح یکپارچگی» را به عنوان «یک مقدار بازنمایی‌کننده خصیصه‌های منحصر به فرد پروژه (به طور مثال، پیچیدگی نرم‌افزار، بحرانی، مخاطره، سطح ایمنی، سطح امنیتی، عملکرد موردنظر، قابلیت اطمینان) تعریف می‌کند که اهمیت نرم‌افزار را برای کاربر تعریف می‌کند»

۳-۴ اصطلاحات مرتبط با شرایط و پیامدها

۱-۴-۳

پیامد

consequence

اثر (با تغییر یا بدون تغییر)، معمولاً مرتبط با یک رویداد یا شرایط یا با سامانه است و معمولاً توسط رویداد، شرایط یا سامانه، مُجاز شده، تسهیل شده، سبب قرار گرفته، ممانعت شده، تغییر داده شده یا مشارکت داده شده است.

یادآوری ۱ مدخل- این امر می‌تواند سودمندی یا خسران باشد یا هیچکدام از آنها نباشد.

۲-۴-۳

مخاطره

risk

ترکیبی محتمل از یک رویداد و پیامد آن است.

یادآوری ۱ مدخل- اصطلاح «مخاطره» معمولاً تنها زمانی که به طور کمینه احتمال پیامدهای منفی باشد به کار می‌رود.

یادآوری ۲ مدخل- در برخی وضعیت‌ها، مخاطرات از احتمال مشتق شدن از برآمد یا رویداد موردانتظار ناشی می‌شود.

یادآوری ۳ مدخل- به استاندارد ISO/IEC Guide 51 برای مسایل مرتبط با ایمنی مراجعه شود.

[منبع: ISO/IEC 16085]

۳-۴-۳

پیامد نامطلوب

adverse consequence

پیامد غیردلخواه مرتبط با خسران است.

۴-۴-۳

پیامد دلخواه (یا مثبت)

desirable (or positive) consequence

پیامد مرتبط با سود یا به دست آوردن یا ممانعت از پیامد نامطلوب است.

۵-۴-۳

خطا

error

حالتی از غلط‌های سامانه است.

۶-۴-۳

اِشکال

fault

نقص در سامانه یا بازنمایی سامانه است که اگر اجرا یا فعال شود، می‌تواند به طور بالقوه منجر بـه یـک خطـا شود.

یادآوری ۱ مدخل- اِشکالات می‌توانند در ویژگی‌ها زمانی که ویژگی‌ها صحیح نباشند، رخ دهند.

۷-۴-۳

حمله

attack

اقدام بدخواهانه یا تعاملی با سامانه یا محیط آن که دارای بالقوگی منجر شدن به یک اِشکال یا یـک خطـا را دارد (و بنابراین محتملاً منجر به توقف) یا یک پیامد نامطلوب می‌شود.

۸-۴-۳

عدول

violation

رفتار، عمل یا رویداد منحرف شده از خاصیت دلخواه سامانه یا ادعای موردنظر است.

یادآوری ۱ مدخل- در حوزه ایمنی، واژه «عدول» به منظور ارجاع به عدول تعمدی انسان از یک رویه یا قاعده است.

۹-۴-۳

توقف

failure

پایان‌دهی به توانایی سامانه در انجام کارکردی ضروری یا ناتوانی آن در انجام داخـل حـدود مشـخص قبلـی است؛ یک انحراف مشهود به طور خارجی از ویژگی سامانه است.

۱۰-۴-۳

توقف نظام‌مند

systematic failure

توقف مرتبط به روشی قطعی با علتی قطعی است که می‌تواند تنها توسط یک اصلاح طراحی یا توسط فرایند سازنده، رویه‌های عملیاتی، مستندات یا عوامل مرتبط دیگر برطرف شود.

۵-۳ اصطلاحات مرتبط با سازمان

۱-۵-۳

سازمان

organization

شخص یا گروهی از مردم و تسهیلات با ترتیبی از مسئولیت‌ها، مراجع و ارتباطات است.

یادآوری ۱ مدخل- مجموعه اشخاص سازمان‌یافته برای برخی مقاصد خاص از قبیل مجمع، اتحادیه، شرکت یا جامعه، سازمان هستند.

یادآوری ۲ مدخل- قسمت شناخته شده‌ای از سازمان (حتی کوچکتر از یک جزء واحد) یا یک گروه شناخته شده از سازمان‌ها می‌تواند اگردارای مسئولیت‌ها، مراجع و ارتباطات باشد، به عنوان یک سازمان مورد ملاحظه قرار گرفته شود.

[منبع: استاندارد ISO/IEC 15288:2008]

۳-۵-۲

مرجع تأیید

approval authority

شخص (یا اشخاص) و یا سازمان (یا سازمان‌های) مسئول برای تأیید فعالیت‌ها، فرآورده‌ها و دیگر جنبه‌های سامانه در طی چرخه عمر آن است.

یادآوری۱ مدخل- مرجع تأیید ممکن است شامل هستارهای متعددی از جمله اشخاص یا سازمان‌ها شود. این امر می‌تواند شامل هستارهای مختلفی با سطوح مختلف تأیید و یا حوزه‌های مختلف موردنظر شود.

یادآوری ۲ مدخل- در وضعیت‌های دو طرفه، مرجع تأیید اغلب متکی به کارفرمایان است. در وضعیت‌های مقرراتی، مرجع تأیید ممکن است طرف سوم از قبیل سازمانی دولتی یا نماینده آن باشد. در وضعیت‌های دیگر برای مثال، فروش محصولات آماده فروش توسعه یافته توسط یک طرف مستقل به مرجع تأیید می‌تواند مسأله مرتبطی با کارفرما باشد.

۳-۵-۳

مرجع طراحی

design authority

شخص یا سازمانی که مسئول طراحی محصول است.

۳-۵-۴

مرجع تضمین یکپارچگی

integrity assurance authority

شخص یا سازمان مستقل مسئول صدور گواهی انطباق با نیازمندی‌های سطح یکپارچگی است.

یادآوری ۱ مدخل- پذیرفته شده از استاندارد ISO/IEC 15026:1998، که در آن تعاریف عبارتند از:« شخص یا سازمان مستقل مسئول ارزشیابی انطباق با نیازمندی‌های یکپارچگی».

۴ ساختار این استاندارد

بند ۵ این استاندارد، مفاهیم پایه از قبیل تضمین، سودبران، سامانه‌ها و محصولات، عدم‌قطعیت و پیامد را پوشش می‌دهد. بند ۶ برخی مسائلی که کاربران قسمت دوم، سوم وچهارم این مجموعه استاندارد نیاز به آگاه شدن از آن دارند را پوشش می‌دهد. بندهای ۷، ۸ و ۹ به‌ترتیب، اصطلاحات، مفاهیم و عناوینی که به طور اختصاصی مرتبط با کاربران قسمت دوم، سوم و چهارم هستند را پوشش می‌دهد، اگرچه کاربران یک

قسمت، می‌توانند از برخی اطلاعات در این بندها برای قسمت‌های دیگر بهره ببرند. ارجاع به اقلام شمارشی در کتاب‌نامه در داخل براکت نمایش داده شده است.

۵ مفاهیم پایه

۵-۱ مقدمه

این بند مفاهیم و واژگان بنیادی تمام قسمت‌های این مجموعه استاندارد را پوشش می‌دهد.

۵-۲ تضمین

این مجموعه استاندارد، از تعاریف خاصی برای تضمین استفاده می‌کند که مبنایی را برای وثوق سنجیده فراهم می‌آورد. عموماً سودبران نیاز به مبنایی برای وثوق سنجیده قبل از اتکا به یک سامانه دارند علی‌الخصوص سامانه‌ای که دارای پیچیدگی، نوآوری، یا فناوری با سابقه اشکالات (به طور مثال، نرم‌افزار) است. هرچه درجه اتکا بیشتر باشد، نیاز بیشتری برای وثوق سنجیده است. لازم است استدلال‌ها و شواهد معتبر مناسب به منظور ایجاد مبنای منطقی برای وثوق سنجیده در ادعاهای مرتبط درمورد خواص سامانه وجود داشته باشد. این خواص ممکن است شامل برخی جنبه‌ها همانند هزینه‌های آتی، رفتار و پیامدها باشد. در سراسر چرخه حیات، باید مبنای کافی برای توجیه تصمیم‌های مرتبط به منظور تضمین طراحی و تولید یک سامانه مکفی و توانایی برای اتکا آن سامانه وجود داشته باشد.

تضمین، اصطلاحی است که کاربرد آن در بین جوامعی که از این اصطلاح استفاده می‌کنند، متغیر است. با این حال، تمامی کاربردها با گذاشتن حدود بر روی عدم قطعیت یا کاهش آن در مواردی مانند سنجش‌ها، مشاهدات، تخمین‌ها، پیش‌بینی‌ها، اطلاعات، تداخلات یا اثرات ناشناخته‌ها مرتبط هستند که هدف نهایی آن‌ها دست‌یابی به یک ادعا و یا نشان دادن آن است. چنین کاهش در عدم قطعیت، می‌تواند مبنای بهبودیادفته‌ای برای وثوق سنجیده ارائه کند. حتی اگر تخمین مقدار خاصیت تغییر نکند، تلاش صرف شده برای کاهش مقدار عدم‌قطعیت، می‌تواند اغلب منجر به اثربخشی هزینه شود زیرا عدم‌قطعیت کاهش‌یافته، مبنای تصمیم‌گیری را بهبود می‌بخشد.

تضمین ممکن است مرتبط با (۱) سامانه یا نرم‌افزارِ مشخص شده‌ای باشد که نیازها و انتظارات دنیای واقعی را مرتفع سازد، (۲) سامانه ساخته شده یا در حال بهره‌برداری باشد که با ویژگی‌ها انطباق دارد، یا هر دو مورد (۱) و (۲) باشد. ویژگی‌ها ممکن است بازنمایی‌هایی از جنبه‌های ایستا و یا پویای سامانه باشند. ویژگی‌ها اغلب شامل توصیف قابلیت، کارکردها، رفتار، ساختار، خدمت و مسئولیت، از جمله جنبه‌های مرتبط با زمان و مرتبط با منبع و همچنین حدودی بر بسامد یا اهمیت انحرافِ محصول و عدم‌قطعیت‌های مرتبط هستند.

ویژگی‌ها ممکن است دستورالعمل و یا محدودیت‌ها (به طور مثال برای رفتار محصول و بر روی رفتار محصول) باشد و همچنین ممکن است شامل سنجه‌های به جا و راهنماهایی برای سبک سنگین کردن باشد.

عموماً ویژگی‌ها، محدودیت‌هایی را برای هنگام کاربست اعمال می‌کنند، مانند محیط و شرایط آن (مثلا دما)، و محتملاً شرایط محصول (مثلا سن یا مقدار پوشش).

۵-۳ سودبران

سامانه‌ها و نرم‌افزار در سرتاسر چرخه حیات خود دارای سودبران متعددی هستند که بر روی سامانه و فرایندهای چرخه حیات سامانه تاثیر می‌گذارند یا تحت تأثیر آن قرار می‌گیرند. سودبران ممکن است از سامانه منتفع شوند، از آن خسارت ببینند، محدودیت‌هایی بر آن تحمیل کنند یا در غیر این صورت دارای «نفع» در سامانه باشند و بنابراین کسانی هستند که نیازمندی‌های سامانه را ارائه می‌کنند. سودبران می‌توانند شامل غیرکاربران باشند که ممکن است عملکردشان، نتایج یا سایر نیازمندی‌هایشان تحت تأثیر قرار بگیرد، به طور مثال، آن‌هایی که نرم‌افزارشان بر روی رایانه‌های یکسان یا هم‌شبکه اجرا می‌شود.

نوع دیگری از ذی‌نفع مهم، حمله‌کننده است که به طور قطع محدودیت‌هایی را تحمیل می‌کند یا علایقی دارد که به سامانه مرتبط است. این استاندارد حمله‌کننده را به عنوان ذی‌نفع در نظر می‌گیرد؛ اگرچه برخی در جامعه امنیتی و دیگرجاها، حمله‌کنندگان را «سودبران» در نظر نمی‌گیرند.

سودبران مرتبط که نیازمندی‌هایشان مد نظر قرار می‌گیرد، نه تنها شامل مالکان و کاربران سامانه است بلکه شامل توسعه‌دهندگان و بهره‌بردارانی است که لازم است نیازمندی‌هایشان برای توسعه و بهره‌برداری از سامانه شناسایی شود. سودبران مختلف، بر اساس شرایط و پیامدها، به مبانی وثوق سنجیده در مورد خواصی از سامانه که نیازمندی‌های آن‌ها شناسایی شده است، نیاز دارند.

۵-۴ سامانه و محصول

به‌منظور سازگاری با استانداردهای ISO/IEC 15288 و ISO/IEC 12207، در این استاندارد از اصطلاح «سامانه» استفاده می‌شود. توصیه می‌شود کاربران این استاندارد که بیشتر با استفاده از اصطلاح «محصول» آشنا هستند، به خاطر داشته باشند که «سامانه» شامل محصولات و خدماتی است که نتیجه فرایندها است و همچنین نرم‌افزار و سامانه و عناصر نرم‌افزار و اجزاء آن است. با وجودی که اصولا انگیزه این استاندارد، ملاحظات مربوط به سامانه‌های ساخته دست بشر (یا تا اندازه‌ای ساخته دست بشر) است ولی می‌تواند برای کاهش عدم قطعیت درمورد وابستگی سامانه به پدیده‌های طبیعی نیز به کار رود.

۵-۵ خاصیت

این مجموعه استاندارد، تضمین را به نیازمندی‌های خاصیت سامانه یا محصول نرم‌افزاری مرتبط می‌کند. یک خاصیت ممکن است از جمله یک شرط، یک خصیصه، یک صفت، یک کیفیت، یک نشان اختصاصی، یک سنجش یا یک پیامد باشد. خاصیت ممکن است ثابت یا وابسته به زمان، وضعیت یا تاریخچه باشد. در این مجموعه استاندارد، از یک خاصیت انتظار می‌رود به طور مستقیم یا غیرمستقیم مرتبط با سامانه یا سامانه‌ها باشد و بنابراین دارای نیازمندی‌های مرتبط است.

خواص ممکن است برای آنچه در گذشته بوده‌اند، آنچه در حال حاضر هستند یا آنچه در آینده خواهند بود، دارای نیازمندی‌هایی باشند. عموماً، مورد آخر، مهم‌ترین آنها در این مجموعه استاندارد است. از آنجایی که این موضوع، مستلزم پیش‌گویی آینده است، اغلب دست‌یابی به آن سخت‌ترین و غیرقطعی‌ترین مورد است، بنابراین رفتار و پیامدهای آتی سامانه (به زیربند ۵-۸ مراجعه شود) اغلب موضوع بنیادینی در تضمین آن قلمداد می‌شود.

بیشتر خواص با نیازمندی‌ها، کیفیت‌های سامانه هستند. استانداردها و گزارش‌های متعدد، فهرست‌ها و تعاریف کیفیت‌هایی که می‌توانند موضوع تضمین باشد را ارائه می‌کند از جمله استانداردهای ISO/IEC 9126-1، ISO/IEC 25010 و مجموعه‌ها استانداردهای مرتبط، ISO/IEC 2382-14، ISO/IEC 9241، ISO/TR 18529 و ISO/TS 25238.

این استفاده از اصطلاح «خاصیت» که از اصطلاح «خاصیت» در استاندارد ISO/IEC 25010 گرفته شده، با آن سازگار است و زیرمجموعه‌ای از کاربرد وسیع آن در این استاندارد است. در استاندارد ISO/IEC 25010 خواصی پوشش داده می‌شوند که موروثی یا غیر موروثی، داخلی، خارجی و در حال استفاده یا زمینه‌ای هستند.

تولیدکنندگان و دیگر سودبران ممکن است خواص را از قبیل کارایی و اطمینان‌پذیری الویت‌بندی کنند و مطالعاتی را برای سبک سنگین کردن آنها و نیازمندی‌های مرتبط با آنها انجام دهند. تعداد بسیاری فن برای پرداختن به این سبک سنگین‌ها، از قبیل آنهایی که در [۲۵]، [۶۴]، [۱۲۲] و[۱۵۷] آمده است، ایجاد شده است. برخی اوقات، مشخص ساختن ادعای سطح بالا برای یک خاصیت، نتیجه تحلیل‌ها از جمله مطالعات سبک سنگین کردن‌ها است.

۵-۵-۱ خواص به‌عنوان رفتار

اغلب خاصیت به عنوان رفتار مشخص می‌شود. در طی انجام عملیات، خواص مرتبط با رفتار ممکن است به طور رسمی به عنوان ترکیبی از موارد زیر مشخص شوند:

- محدودیت بر حالت‌های مجاز سامانه (برخی اوقات «خاصیت ایمنی» نامیده می‌شود)
- حالت‌های سامانه که باید بدان دست یافت؛ نیاز به پیشرفت یا به انجام رسانیدن دارند («خاصیت زنده بودن»)
- حدود بر روی جریان‌ها یا تعاملات؛ نیازمندی‌هایی برای حدود جداسازی

این نوع خواص می‌تواند به عنوان شرایط یا حدودی که باید در سامانه صحیح باشند، اظهار شوند.[1] در عمل، این موارد جزیی نبوده و پیمانه‌ای هستند، زمان در آن‌ها دخالت دارد و حالتی (حالت‌هایی) را آغاز می‌کنند و همچنین انتقال به حالتی دیگر را که مرتبط با تعامل با محیط سامانه یا نرم‌افزار است را موجب می‌شوند.

بیشتر انواع جریان‌ها از قبیل گازها، سیالات، عبور و مرور یا اطلاعات می‌توانند مد نظر قرار گیرند و همچنین حدود بر روی آن‌ها از قبیل غیرتداخل‌ها و جداسازی‌ها باید نگهداری شوند. به علاوه، اغلب مرسوم یا لازم است که حدود بر روی جریان تعیین شود تا جنبه‌های امنیت اطلاعات از جمله سازوکارهای کنترل دسترسی و خط‌مشی‌ها و محدودیت بر روی اطلاعات مخابره شده به طور آشکارا یا نهانی مشخص شود [۱۳۵].

۵-۶ عدم قطعیت و وثوق

عدم قطعیت، در این مجموعه استاندارد به عنوان اصطلاحی فراگیر به کار می‌رود. اینمفهوم، فقدان قطعیت را چه بتواند با استفاده از احتمالات مدل‌سازی شود یا خیر، پوشش می‌دهد. عدم قطعیت می‌تواند شامل تصورات مبهمی باشد که بدون استفده از احتمالات بخواهد مدل‌سازی شود. جوامع خاصی، کاربرد این اصطلاح را به پیش‌بینی رویدادهای آتی،سنجش‌های فیزیکی که قبلا انجام شده‌اند، یا ناشناخته‌ها محدود می‌کنند. با وجودی که این کاربردهای محدود، داخل آن جوامع، مرسوم هستند، کاربران این مجموعه استاندارد جوامع بیشتری را پوشش می‌دهند.

درجه وثوقی که می‌تواند مبتنی بر مورد تضمین خاصی به‌طور سنجیده ایجاد شود یا وجود داشته باشد، ممکن است به تناسب شخص یا سازمان و موقعیت متغیر باشد. هر چه عدم قطعیت در مورد ادعاهای مورد تضمین کمتر باشد، میران وثوق سنجیده آن بالاتر است، اگرچه تبدیل میزان عدم قطعیت به درجه‌ای از وثوق سنجیده برای کاربردهای معین سرراست نبوده و به خوبی قابل درک نیست. به این دلیل و دلایل دیگر، برخی اوقات، پیامدها به طور مستقیم داخل مورد تضمین گنجانده می‌شوند. با وجودی که این امر شکاف منطقی را به هم نزدیک می‌کند، نافی عمل تصمیم‌گیرندهٔ در مورد قضاوت مرتبط با درجه وثوق نیست.

۵-۷ شرایط و رویدادهای آغازین

مورد تضمین نیاز به پوشش تمامی شرایط دارد که می‌توانند دارای اثر منفی مهمی بر نتیجه و عدم قطعیت ادعای سطح بالا داشته باشد. دنیای شرایط و رویدادهای مرتبط به طور بالقوه می‌توانند در ابتدا به منظور شناسایی [۲] و معلوم کردن این که کدام یک اثر مهمی دارد که می‌تواند در ابتدا بدون گنجاندن آن‌ها به طور کمینه در مورد تضمین سخت باشد.

۱- اگر به طور رسمی مشخص شود، این موضوع می‌تواند تحلیل ایستای انطباق طراحی‌ها و کد را مجاز کند و به طور بالقوه به شواهد تضمین معتبر بیافزاید.

به طور تاریخی، یک شرطی که بیشترین توجه را دریافت می‌کند، توقف سامانه است. حجم قابل توجهی از بازبینه‌ها[1]، عمل و ادبیات دردغدغه توقف سامانه موجود است (به طور مثال، فصل ۱۸، [۲]، [۷] و [۱۴] صفحات ۴۷۵ الی ۵۲۴) . تا زمانی که بیشتر این کار در جوامعی که ایمنی، امنیت یا خطای انسانی را نشان می‌دهند، انجام شود، توقف سامانه می‌تواند منجر به دست‌یابی کمتری از خاصیت مثبت یا پیامد مثبت و همچنین خواص منفی یا خسارات شود.

خطرناکی رفتار سامانه می‌تواند توسط شرایط محیط آن متفاوت باشد. این رفتارها و شرایط اغلب به منظور تعیین این که پیامد های نامطلوب خواهد بود یا خیر، نیاز به ترکیب در طی تحلیل دارند.

طراحان سامانه خواهان آگاهی از تمامی رویدادهای شرایط داخل محیط هستند یا نیستند؛ اگرچه ممکن است سروکار داشتن شرایط خطرناک نیاز باشد ولو این که نه تمامی رویدادهای آغازین شناخته یا قابل تشخیص باشند.

۸-۵ پیامدها

خارج سامانه، بیشتر دلایل مبتنی بر شرایطی است که می‌تواند منجر به پیامدهای نامطلوب و رویدادهای آغازین آن‌ها یا پیش‌شرط‌ها شود. داخل سامانه، دلایل مبتنی بر شرایطی است که می‌تواند منجر به رفتارهای خطرناک سامانه و رویدادهای آغازین آن یا پیش‌شرط‌ها شود. یک دلیل ممکن است به مورد زیر مرتبط باشد:

پیامد، از منظر، دیدگاه یا موارد مورد نظر ذی‌نفع، دلخواه است یا داخواه نیست. پیامد ممکن است هرجایی در طور عمر سامانه رخ دهد.

در سامانه‌های فنی پیچیده، توضیحات رویدادهای بد یا ادعا تخطی‌ها نمی‌تواند به توقف‌های «اجزا» محدود باشد. پیامدهای نامطلوب می‌تواند برآمده از تغییرپذیری و تعاملات پیش‌بینی نشده یا مورد انتظار رفتار عادی باشد. [۵۷][۵۴] بدون در نظر گرفتن چگونگی برآمدن آن‌ها، شرایط خطرناک و پیامدهای نامطلوب، موضوع کاهش هستند.

حمله‌کنندگان می‌توانند توانایی‌ها، منابع، انگیزه‌ها و شدت‌ها را تحمیل کنند که آن‌ها را قادر می‌سازد تا شروع به کار کنند و تلاش‌های بدخواهانه را به منظور نقض ادعا به دنبال داشته باشند. نقض‌کنندگان، از توانایی‌هایشان در به دست آوردن منافع از فرصت‌های ارائه شده توسط سامانه و یا ارائه شده توسط محیط

1 - checklists

استفاده یم‌کنند که به آن آسیب‌پذیری گویند، از جمله « ضعیف بودن ..... که می‌تواند باعث شود توسط منبع تهدید از فرصت استفاده شود یا راه‌اندازی شود.» [۱۵۰][1].

برخی اوقات نقطه سوءتعبیر، همان است که دغدغه‌هایی است که بدخواهانه و منهدم‌کننده هستند و حتی وقتی که خاصیت مرتبط با امنیت مرتبط نباشد، درگیر می‌کند. توسعه‌دهندگان بدخواه، خواهان تلاشی بر روی دست‌یابی تقریبا موفق هر خاصیتی هستند.

بیشتر استانداردها یا گزارشات، به پیامدهای مرتبط با سامانه‌ها داخل یک دامنه خاص اشاره می‌کنند. مثال‌ها شامل استانداردهای ISO 14620، [۷۹] ISO 19706 و ISO/TS 25238 است. همچنین استانداردهای مدیریت مخاطره، به پیامدهایی را برای مثال، ISO/IEC 16085 [۹۱] و ISO 31000 اشاره می‌کنند.

۶ استفاده از قسمت‌های چندگانه این مجموعه استاندارد

۶-۱ مقدمه

این مجموعه استاندارد یا قسمت‌های آن می‌تواند به تنهایی با استانداردها یا راهنمای دیگر مورد استفاده قرار گیرد. قسمت‌های این مجموعه استاندارد می‌تواند به بیشترین استانداردهای چرخه عمر نگاشت شود و مس‌تواند از هر مجموعه کیفیت‌ها یا خواص‌های به خوبی تعریف شده استفاده کند.

۶-۲ راهنمای کاربرد ابتدایی

خواص و یا ادعاها پوشش داده شده در هنگام استفاده از این مجموعه استاندارد، سراسر بسته به کاربران استانداردی است که پاسخ‌گو نیازها و نیازمندی‌های ذی‌نفع سامانه است. هرگونه خاصیت یا ادعا ممکن است برای مورد تضمین بدون در نظر گرفتن مهمی آن یا مخاطره مرتبط با آن انتخاب شود؛ اگرچه قسمت‌های این مجموعه استاندارد در ابتدا برای آن خواصی یا خاصیت اصلی‌تری که ذی‌نفع آن را مهم می‌پندارد طراحی می‌شود. قسمت چهارم این مجموعه استاندارد، از اصطلاح «خواص حیاتی» برای این الویت‌ها و نیازمندی‌ها استفاده می‌کند.

تا زمانی که به طور کلی قسمت سوم این مجموعه استاندارد، سازگار با نسخه قبلی استاندارد ISO/IEC 15026:1998 در گذار به قسمت سوم این مجموعه استاندارد باشد، نیاز به بررسی برخی تغییرات خواهد بود. قسمت سوم این مجموعه استاندارد، بحث مهندسی جدید و گزینه‌های تصمیم‌گیری را بازکرده است چرا که تنها نه منظری مستقل است بلکه همچنین شامل سطوح یکپارچکی مرتبط با مورد تضمین است. قسمت

۱- برای بیشتر مقاصد، می‌تواند معنادار بودن و نیاز به جداسازی آسیب‌پذیری‌ها از ضعف‌های دیگر، وجود نداشته یا کمتر باشد. به علاوه، یک سوال همیشه در مورد زمینه‌های فعلی و آتی موجود است که به فرصتی که «می‌تواند از آن استفاده کند یا راه‌اندازی کند» مرتبط است.

سوم این مجموعه استاندارد، بیشتر بر روی خود سامانه و سطوح یکپارچگی به جای تحلیل مخاطره خارجی تمرکز دارد و همچنین شامل ایجاد سطوح یکپارچگی است. بند ۸ در مورد سطح یکپارچگی بحث می‌کند.

۳-۶ ارتباطات میان قسمت‌های این مجموعه استاندارد

قسمت‌های این مجموعه استاندارد به شرح زیر هستند:

قسمت اول این مجموعه استاندارد، *مفاهیم واژگان، مفاهیم و اصطلاحات را به عنوان مبنای تمام قسمت‌های این مجموعه استاندارد توضیح می‌دهد.*

قسمت دوم این مجموعه استاندارد، *مورد تضمین، شامل نیازمندی‌های محتوا و ساختار مورد تضمین است.*

قسمت سوم این مجموعه استاندارد، *سطوح یکپارچگی سامانه، سطوح یکپارچگی به مورد تضمین مرتبط می‌کند و شامل نیازمندی‌ها جهت استفاده آنها با مورد تضمین یا بدون مورد تضمین است (تجدیدنظر ISO/IEC 15026:1998)*

قسمت چهارم این مجموعه استاندارد، *تضمین در چرخه عمر، راهنما و توصیه‌نامه‌های مرتبط با تضمین را برای فعالیت‌های خاص در سراسر فرایندهای سامانه و چرخه عمر نرم‌افزار ارائه می‌کند.*

تا زمانی که قسمت دوم، قسمت سوم و قسمت چهارم این مجموعه استاندارد، عناوین تضمین را به طور جداگانه ارائه می‌کند و ممکن است به تنهایی به کار روند، آن‌ها ممکن است باهم به کار روند چرا که آن‌ها مجموعه‌ای مرتبط را شکل می‌دهند. این استاندارد، پس‌زمینه، مفاهیم و واژگان را ارائه می‌کند که در تمام هر سه کاربردپذیر است و مقدمات خاصی جهت پوشش این سه قسمت از مجموعه استاندارد است.

مورد تضمین، چه بیشتر یا کمتر مرتبط با تمامی قسمت‌ها است اگرچه قسمت چهارم این مجموعه استاندارد، دست‌یابی به ادعا را مورد بحث قرار می‌دهد و دست‌یابی ادعا را نشان می‌دهد چه صورت پذیرد چه صورت نپذیرد، «نشان دادن، در فرآورده که خصوصاً «مورد تضمین» نامیده می‌شود، گنجانده می‌شود.

قسمت دوم این مجموعه استاندارد، بر روی محتواها و ساختار مورد تضمین متمرکز است. قسمت سوم این مجموعه استاندارد، سطوح یکپارچگی و موارد تضمین را با توصیف چگونگی توانایی کار سطوح یکپارچگی و موارد تضمین باهم مخصوصاً در تعریف ویژگی‌های سطوح یکپارچگی یا توسط استفاده از سطوح یکپارچگی داخل سهمی از مورد تضمین، مرتبط می‌کند. این ارتباط تحت تابع درجه مخاطره و وابستگی‌ها در سامانه است.

اگر مخاطرات یا برطرف کردن مخاطره، به خوبی درک نشود یا اگر ساختار وابستگی کل سامانه یا انتخاب ادعاهای مناسب شفاف نباشد، سپس استفاده از مورد تضمین از استفاده از سطوح یکپارچگی گزینه بهتری است. بالاخص این امر موردی است که با انواع مخاطرات جدید مواجه می‌شود یا از انواع برطرف‌سازی‌های جدید استفاده می‌کند.

زمانی که مخاطرات و برطرف‌سازی آن‌ها به خوبی درک شوند، اگرچه توسعه‌دهندگان نیاز به توجیه انتخاب ادعای سطح بالا ندارند و تنها نیاز به انتخاب ادعاهای مناسب در زمینه خود از مجموعه شناخته شده دارند – یک سطح یکپارچگی از یک مجموعه سطوح یکپارچگی. در این وضعیت، استدلال‌های عام ایجاد شده توسط تعریف‌کنندگان سطح یکپارچگی، توجیهی را که نیازمندی‌های سطح یکپارچگی را مرتفع می‌سازد، ارائه می‌کنند و به قدر کفایت مرتفع‌سازی سطح یکپارچگی را نشان خواهند داد. یک چنین توجیهی (بهطور مثال، مورد تضمین تعمیم داده شده) معمولاً یکباره توسط سازمان جداگانه ایجاد شده و توسط پروژه‌های متعددی به کار می‌رود.

قسمت چهارم این مجموعه استاندارد، شامل راهنما و توصیه‌نامه‌های مرتبط با تضمین برای فعالیت‌ها میان فرایندهای چرخه عمر است از جمله فعالیت‌هایی که ورای آن دسته ادامه می‌یابد که به طور مستقیم مرتبط با یک مورد تضمین است، به طور مثال، طرح‌ریزی پروژه برای مصالح مرتبط با تضمین.

۴-۶ مراجع

قسمت‌های این مجموعه استاندارد همان طور که در بند ۳، اصطلاحات و تعاریف تعریف شده، مشمول مراجع هستند. برای مثال، قسمت سوم این مجموعه استاندارد، شامل به دست آوردن توافقات بین مرجع طراحی و مرجع تضمین یکپارچگی هستند. به علاوه، سامانه جدید نیاز به موزهای تأیید شده از کارفرما دارد تا مسئولیت فرایند ایجاد موارد تضمین را با مرجع طراحی و مرجع تضمین یکپارچگی تأمین‌کنندگان برعهده گیرد.

اگرچه، «مرجع تأیید شده» برای مورد تضمین ضرورتاً توجیه متابعت با قسمتی از این مجموعه استاندارد را ندارد. ادعاهای ممکن از تبعیت با قسمت‌های استاندارد، به جای کیفیت فرآورده‌ها و تصمیمات توجیهی در زمینه سامانه یا پروژه، بر جنبه‌هایی توجیه می‌شوند که به منظور مناقشه صریح و سخت‌تر هستند. در عمل، قراردادها می‌تواند به طور صریح کارفرمایان مستلزم کند تا مرجع تأیید بدهند یا تأییدکننده تبعیت با قسمت‌های این مجموعه استاندارد باشند.

۷ این مجموعه استاندارد و مورد تضمین

۱-۷ مقدمه

قسمت دوم این مجموعه استاندارد، ساختار ومحتوای یک مورد تضمین را پوشش می‌دهد و ۵ جزء اصلی مورد تضمین را توصیف می‌کند: ادعاها، استدلالات، شواهد، توجیه‌ها و مفروضات. هدف یک مورد تضمین، بهبود ارتباطات تضمین با آگاه‌دهی به تصمیم‌گیری سودبران و تأمین موجبات برای اطمینان مودرنیاز ذی‌نفع است. رایج‌ترین استفاده از مورد تضمین، ارائه تضمین در مورد خواص سامانه نسبت به طرفین است که نه

دقیقاً در فرایندهای توسعه فنی سامانه مشمول می‌شود. این قبیل طرف‌ها ممکن است در صدور گواهی[1] یا، مقررات، اکتساب یا ممیزی[2] درگیر باشند. معمولاً یک مورد تضمین دلایل انتظار و تأیید تولید موفق سامانه را از جمله احتمالات و مخاطرات شناسایی شده همانند سختی‌ها یا موانع را به منظور توسعه و ابقاء آن سامانه نشان می‌دهد.

برخلاف اثبات‌های منطقی از اثبات قیاسی از ادعاهای برگرفته از شواهد که جنبه‌های حقیقت مطلق یا جنبه‌های حقیقت افلاطونی را پوش می‌دهند، موارد تضمین با جنبه‌های روش‌های جدلی سامانه که حقیقت همیشه مرتبط یا حتی غیرعینی است. به بیان دیگر اثبات‌های منطقی تحت نظریه منطقی ثابتی توصیف می‌شوند ولی موارد تضمین ممکن است بر مبنایی که نظریه منطقی اصلی آن نامناسب است، رد شود. نیاز برای مورد تضمین زمانی که یک مورد که خواص سامانه را در دنیای واقعی محقق ساخته نتواند به طور کامل در نظریه منطقی رسمی شود، به وجود می‌آید ولی همیشه چیزی وجود دارد که توسط هرگونه رسمی‌سازی منطقی پوشش داده نمی‌شود.

یادآوری- زمانی که ادعای سطح بالا در مورد ایمنی، امنیت، وابسته‌پذیر بودن یا (اطمینان‌پذیری، دسترس‌پذیر بودن و نگهداشت‌پذیری) (RAM)[3] باشد، موارد تضمین مرتبط با این ادعاها به ترتیب موارد ایمنی، موارد امنیتی، موارد وابستگی‌پذیری یا موارد RAM نامیده می‌شوند. به [۱۳۹]، [۱۴۲]، [۱۴۳]، [۱۴۶]، [۱۵۴]، [۱۵۵]، [۱۶۸]، [۷۴]، [۲۲]، [۲۳] و [۲۴] در کتاب‌نامه مراجعه شود.

همانند یک فرآورده مطرح شده، مورد تضمین دارای جنبه‌های مرتبط با کیفیت همانند ماهیت محتوا، شکل یا ساختار آن (به طور مثال، روش یا استدلال یا پودمانی)، مسائل معنایی از قبیل کامل شدن، ایجاد و نگهداشت از جمله پشتیبانی ابزار، کاربست‌پذیری و ارائه، یکپارچگی، اعتبار، قابلیت درک و دارای نتیجه‌گیری بیان شده شفاف با درجات صریح عدم قطعیت است. یک مقاله [۱۶۴] فهرست معتبری از خصیصه‌های مرتبط با کیفیت برای موارد تضمین را پوشش می‌دهد. جنبه‌های مرتبط با کیفیت یک مورد تضمین در قسمت دوم این مجموعه استاندارد یا دیگر قسمت‌های این مجموعه استاندارد پوشش داده نشده است.

هرگونه اصلاحات ماهوی در سامانه، تغییرات در محیط یا تغییرات در ادعاهای سطح بالای مورد تضمین وادار به ثبت تغییرات در مورد تضمین می‌کند. بنابراین یک مورد تضمین معمولاً شامل مجموعه شواهد در حال گسترش ترقی‌خواهانه ایجاد شده در طی فعالیت‌های چرخه عمر توسعه و بعدتر هستند که همان‌طور که برای تمامی تغییرات مرتبط مورد نیاز هستند، واکنش نشان می‌دهند. [صفحه ۵ از [۱۳۹]].

1 - certification
2 - audit
3 - reliability, availability and maintainability

یادآوری- ادعا(های) موارد تضمین بر مقادیری که می‌تواند شامل کل مجموعه نیازمندی‌های سامانه برای یک خاصیت موردنظر شود، است. یک مثال می‌تواند ادعای سطح بالایی داشته باشد که متشکل از (۱) حدود موردنیاز بر پیامدها (۲) کارکردپذیری و خود خواص سامانه (به طور مثال، که این کارکردپذیری نمی‌تواند مورد قبول واقع شود). کیفیت‌های تعریف شده در مجموعه استانداردهای ISO/IEC 25000 شامل کیفیت‌های مرتبط با کارکردپذیری و حدود است. معیار رایج تجدیدنظر ۲ نسخه ۳.۱ [۳۰] همچنین در هردو علاقه دارد.

۲-۷ توجیه روش برهان

یک استدلال دارای یک توجیه مرتبط برای اعتبار یا شایستگی روش برهان خود است. روش استدلال می‌تواند منبع افزوده عدم قطعیت باشد.

تنوع مبناهای استدلال و تحلیل در مورد تضمین می‌تواند به کار رود و این امر در کاربست‌پذیری، قدرت، نتیجه دقت و عدم قطعیت، سهولت در استفاده از آن‌ها متغیر است. موضوعات و دست‌یابی به برهان، در میان جوامعی که دارای انگیزش‌ها، فضاهای فکری متفاوت و اغلب دارای روش‌های متعدد برهان هستند، متفاوت است.

مثال‌هایی از روش‌های برهان شامل موارد زیر است:

- کمی:
  - جبری (به طور مثال، اثبات‌های رسمی)
  - سامانه‌های رسمی غیرجبری برای برهان
  - احتمالات
  - نظریه بازی (به طور مثال، minimax[۱])
  - سامانه‌های رسمی مبتنی بر عدم قطعیت دیگر برهان (به طور مثال، مجموعه‌های فازی)
- کمی (به طور مثال، ارزیابی‌های عملکرد کارکنان، توجیه‌های محکمه‌ای و اظهارات کیفی علیت رویداد محصولات و شرایط پیچیده – و هر انسان مشمول آن- به منظور ایجاد کمَی پیش‌بینی‌های دقیق و صحیح، فرای حالت فعلی صنعت هستند. توجیه‌های غیرعینی در عدم حضور فنون و روش‌های مقرون به صرفه، مناسب و عینی‌تر یا جایی که نیاز به متمم یا ارزیابی نتایج این چنین فنون باشد، به کار می‌رود. فنون کمی الحاقی متمم با بازنگری و توجیه خُبره، به طور گسترده به کار می‌رود و عموماً پذیرفته می‌شود. همانند دیگر شکل‌های استدلال، توجیه‌های غیرعینی شکل ادعا و پشتیبانی آن را به خود می‌گیرند. تا زمانی که برخی

۱- یک قاعده تصمیم‌سازی است که در نظریه تصمیم، نظریه بازی‌ها، آمار و فلسفه برای کمینه کردن احتمال شکست و ضرر در بدترین حالت (بیشترین احتمال ضرر) از آن استفاده می‌شود.

اوقات ضرورت یا سود داشته باشد، توجیه‌هایغیرعینی داخل مورد تضمین می‌تواند منجر به غیرقطعیات افزوده شود یا عموماً (فقط به طور فرض) با بحران کمتر، توجیه بهتر است.

الگوهای رخ‌دادهای رویدادهای «طبیعی» و رفتارهای رایج، غیربدخواهانه انسانی معمولاً به طور احتمالی توصیف می‌شود. اگرچه، احتمالات برای فعالیت‌های هوشمندانه، بدخواه که احتمال آن قابل تعیین یا شناخته شده نیست، خصوصاً دغدغه است، اگر فعالیت‌های هوشمندانه، بدخواه متخاصم به طور عمد به هر احتمالی که می‌تواند عطف به رفتارشان آن را ارزیابی کند، به طور مثال، غافل گیر کردن، آسیب رساند. این تمایز در تفاوت برهان بین ایمنی و امنیت مرکزی است.

۳-۷ ابزار دست‌یابی به شاهد و مدیریت شواهد آن

برای هر خاصیت، ابزارهای زیاد در دست یابی شواهد موجود است. در میان این ابزار، تجربیات انسانی، تاریخچه، مشاهدات، سنجش‌ها، آزمون‌ها، نتایج ارزیابی و انطباق، تحلیل‌ها، نقایص و تداخلات وجود دارد. شواهد می‌تواند به عینیات ادعا شده در استدلال تضمین را دست یابد (MoD DefStan 00- قسمت سوم – بخش ۹-۱ [۱۳۹])

مجموعه شواهد می‌تواند کاملاً عظیم باشد و ممکن است نیاز به سازمان‌دهی و مدیریت توسط برخی چارچوب‌های ارائه‌کننده عملکرد و قابلیت ردیابی شواهد باشد تا ارائه به کاربران نسبت به منبع، محتوا و اعتبار خود اطمینان دهد. یک کتاب راهنما موارد زیر را نشان می‌دهد[۱۵۰]:

- توصیه می‌شود شواهد به طور منحصر به فرد شناسایی شوند که استدلالات بتوانند به طور منحصر به فرد به شواهد اشاره کند.
- توصیه می‌شود شواهد قابل تصدیق و ممیزی باشد
- توصیه می‌شود شواهد توسط مدیریت پیکربندی محافظت و کنترل شود
- شواهد نیاز به تکمیل توسط فراداده‌هایی که در به کاربردن مناسب آن داخل مورد تضمین موردنیاز است.

این نکات آخر به سادگی بازاظهاری از آنچه گمان می‌رود آزمون، مرتبط با مورد تضمین به دست آورد، است.

۴-۷ صدور گواهی و اعتباردهی

همه جنبه‌ها دارای پیامدهای مهم بالقوه برای مرتفع‌سازی ادعای سطح بالا یا برای اطمینان داشتن از این که سودبران کلیدی دارای جایگاه بالقوه‌ای در شواهد کامل مورد تضمین داشته باشند، هستند. توصیه می‌شود این امر نه تنها اطمینان منسجمی به سودبران می‌دهد بلکه همچنین دارای اطلاعات کافی جهت استفاده توسط صادرکنندگان و اعتبارگذاران است.

صنایع هواپیمایی و انرژی هسته‌ای دارای تاریخچه‌های طولانی استانداردها و صدور گواهی‌ها هستند و جامعه امنیتی در استاندارد ISO/IEC JTC 1/ SC 27 در مورد عناوین تضمین برای سال‌های زیادی کار کرده شده

است. مثال‌های از امنیت شامل معیارهـای رایـج FIPS 140 بـرای رمزنگـاری[1] و ISO/IEC 27002، *فنـاوری اطلاعات، آیین کار مدیریت امنیت اطلاعات* در ترکیـب بـا ISO/IEC 27001 (قـبلاً بـا اسـتاندارد انگلیسـی BS 7799-2:2202) صدور گـواهی سـامانه عملیـاتی. وزارت دفـاع انگلـیس و سـازمان هواپیمـایی کشـوری همچنین استانداردهای موردنظر از جمله استانداردهای مبتنی بر مـورد تضـمین را بـرای قابلیـت اطمینـان، نگهداشت‌پذیری و ایمنی تولید کرده است – به طـور مثـال، [۱۳۹]، [۱۴۲]، [۱۴۳]، [۲۲]، و [۲۳]. بیشـتر استانداردها در کتاب‌نامه فهرست شده است.

جامعه ایمنی (به طور مثال، هواپیمایی بخش خصوصی) از صدور گواهی کارکنـان کلیـدی (عمـل یـا پروانـه تعیین شده) به عنوان قسمتی رویکرد خود به کار برده است. تعدادی صدور گواهی ایمنی و امنیـت رایانـه از نمونه‌های مدیریت‌گرایی به نمونه‌های فنی در مورد تولیدات خاص، به طور مثال، صدور گواهی از کنسرسیوم صدور گواهی امنیت سامانه‌های اطلاعات بین‌المللی (ISC)[2] و انستیتو SANS موجود است.

۸ این مجموعه استاندارد و سطوح یکپارچگی

۸-۱ مقدمه

سطوح یکپارچگی برای استفاده در سطوح قطعی مخاطره یا پشـتیبانی از یـک مـورد تضـمین و تحمیـل آن خصوصاً بر روی پروژه، شواهد جمع‌آوری شده و سامانه مناسب است. یک سطح یکپارچگی می‌تواند به عنوان بازنمایی از درجه اطمینانی که به منظور دست‌یابی توافق در میان سودبران سامانه در مورد مخاطرات مرتبط با آن سامانه به کار رود، دیده شود.

در ابتدا قسمت سوم این مجموعه استاندارد، یک چـارچوب سـطح یکپـارچگی را ایجـاد مـی‌کنـد. در ادامـه استاندارد، تعریف سطوح یکپارچگی را با استفاده از سطوح یکپارچگی و با تعیین سطح یکپارچگی سامانه یـا محصول با استفاده از تحلیل‌های مخـاطره، بـا تخصـیص سـطوح یکپـارچگی جـزء سـامانه و بـرآورده‌سـازی نیازمندی‌های سطح یکپارچگی با استفاده از شواهد و توافقات و تأییدهای همراه با مرجع (طبق زیربند ۶-۴) پوشش می‌دهد.

نیازمندی‌های سطح یکپارچگی آنچه موردنیاز برای دست‌یابی و نشان دادن آن که سـامانه یـا جـزء سـامانه، خواص ادعا شده توسط سطح یکپارچگی خود را دارد، داشته و یا خواهـد داشـت را بازتـاب مـی‌کنـد. سـطح یکپارچگی سامانه آنچه برحسب خواص کل سامانه کفایت می‌کند را اظهار مـی کنـد. بنـابراین، نشـان دادن خواص، نقش مبنایی در نشان دادن مرتفع‌سـازی ادعاهـای بزرگتـر مشـمول سـامانه و محـیط آن از جملـه پیامدهای دلخواه یا غیر داخواه دارا است. اگر این قبیل ادعاهای بزرگ ایجاد نشود، دست‌یابی و نشـان دادن

1 - cryptography
2 - International Information Systems Security Certification Consortium

سطوح یکپارچگی جزء سامانه، قسمت مبنایی از نشان دادن ادعای سطح بالا را عطف به خود سامانه تأمین می‌کند.

یادآوری- سطوح یکپارچگی و استانداردهای بهره‌برداری کننده از آن‌ها دارای تاریخچه مهمی به خصوص در ایمنی هستند. سطوح یکپارچگی در استانداردهای مرتبط با ایمنی در مجموعه‌های سطح چندگانه با نشان داده درجه‌های متنوع شدت و یا عدم قطعیت دست‌یابی آن‌ها با سطوح بالاتر با ارائه کردن شدت بالاتر و عدم قطعیت کمتر تعریف می‌شوند. مثالی از استاندارد ایمنی، استاندارد IEC 61508، *ایمنی کارکردی سامانه‌های مرتبط باالکتریک/ الکترونیکی / الکترونیکی /برنامه‌نویس الکترونیکی* [۷۰]. به عبارت دیگر، طرح‌واره‌های مشابه با برچسب‌هاب متفاوت به کار می‌روند، به طور مثال، «رده‌های انطباق».

۲-۸ تحلیل مخاطره

تحلیل مخاطره، سطح یکپارچگی موردنیاز را برای کل سامانه ایجاد می‌کند. تحلیل مخاطره فرایند مداوم و تکرارشونده است که توصیه می‌شود آنچه را که هنوز شناخته نشده است با آنچه را نیاز به شناختن دارد متعادل کند. سطوح یکپارچگی برآمده از تحلیل‌های مخاطره، ترجمه مقادیر پیامدها به رخدادها و زمان‌بندی شرایط یا رفتارهای سامانه است. این ترجمه به داخل سطوح یکپارچگی سامانه و وابستگی‌های آن منتشر می‌شود همان‌طور که آن‌ها همچنین برچسب رخدادها و زمان‌بندی‌ها هستند. بنابراین، سطوح یکپارچگی، آنچه که موردنیاز برای انجام و نشان دادن برای گستره و شدت‌های متنوعی از حدود بر روی مقادیر خاصیت و عدم قطعیت مرتبط به آنها است را تدوین می‌کند.

این مجموعه استاندارد تحلیل مخاطر را به تفصیل پوشش نمی‌دهد. بیشتر استانداردها و مستندات راهنمایی موجود هستند که پیشنهاد راهنماهایی برای تحلیل مخاطره می‌دهند و می‌توانند به شناسایی پیامدهای نامطلوب بالقوه کمک کنند. استاندارد IEC 61508 [۷۰] و استاندارد IEC 31010 ویرایش اول سال ۲۰۰۹، *مدیریت مخاطره، فنون مدیریت مخاطره*، رویکردهایی را به منظور تحلیل مخاطره ارائه می‌کنند. در نتیجه استفاده مجموعه اصطلاحات خاص در ایمنی در استاندارد IEC 300-3-9، توصیه می‌شود اصطلاحات «در معرض خطر قرار گرفتن»[1] و «خسران»[2] به ترتیب به عنوان «شرایط خطرناک» و «پیامد نامطلوب» ترجمه می‌شود. استاندارد 60300، *مدیریت وابستگی‌پذیری*، [۶۴] همچنین راهنمایی ارائه می‌کند.

استانداردهای تخصصی دیگر شامل استاندارد ISO 13849 [۷۸] در مورد ماشین آلات، استاندارد ISO 14620 [۷۹] در مورد سامانه‌های فضایی، استاندارد ISO 19706 [۸۱] درمورد حریق، استاندارد ISO/TS 25238 [۱۲۱] در مورد انفورماتیک سلامت، استاندارد ISO/IEC 27005 [۱۱۰] در مورد امنیت اطلاعات و استاندارد UK CAP 760 [۲۴] در مورد ترافیک هوایی و فرودگاه‌ها است. همچنین علاقه‌های محتمل می‌تواند استانداردهای بیشتر عمومی مدیریت مخاطره ISO/IEC 16085 [۹۱] و استاندارد ISO 31000 باشد.

1 - hazard
2 - harm

۹ این مجموعه استاندارد و چرخه عمر

۹-۱ مقدمه

قسمت چهارم این مجموعه استاندارد، *تضمین در چرخه عمر*، یک دید *فرایند* برای تضمین سامانه‌ها و نرم‌افزار توسط ارائه اظهارنامه‌ای از هدف و مجموعه‌ای از برآمدهای مناطب برای تضمین سامانه‌ها و نرم‌افزار، ارائه می‌کند. مفهوم دید فرایند، در پیوست استاندارد ISO/IEC 15288، *مهندسی سامانه‌ها و نرم‌افزار – فرایندهای چرخه عمر سامانه*، فرمول‌بندی و توصیف شده است. برخلاف فرایند، توصیف دید فرایند مشمول فعایت‌ها و وظایف نمی‌شود. در عوض، توصیف شامل راهنما و توصیه‌هایی است که چگونگی دست‌یابی به برآمدها را توسط به کارگیری فعالیت‌ها و وظایف فرایندهای مختلف در استانداردهای ISO/IEC 15288 و ISO/IEC 12207، *مهندسی سامانه‌ها و نرم‌افزار – فرایندهای چرخه عمر نرم‌افزار* توضیح می‌دهد.

تمام فرایندهای چرخه عمر در هر دو استاندارد ISO/IEC 15288 و ISO/IEC 12207 تعریف شده است اگرچه فرایندها در استاندارد ISO/IEC 12207 برای نرم‌افزار اختصاصی شده است و در برخی موارد دارابینام‌های متفاوتی است که تخصصی بودن را بازتاب می‌دهد. استاندارد ISO/IEC 12207 شامل فرایندهایی است که در استاندارد ISO/IEC 15288 گنجانده نشده است و مرتبط با فرایندهای پیاده‌سازی نرم‌افزاراست؛ که از فرایندها پشتیبانی کرده و از فرایندها بازاستفاده می‌کند.

فرایندها، فعالیت‌ها، وظایف و راهنما و توصیه‌ها تماماً باید در زمینه مدل چرخه عمر انجام شود. گزارش فنی چندبخشی استاندارد ISO/IEC/TR 24748، *مهندسی سامانه‌ها و نرم‌افزار – مدیریت چرخه عمر* به منظور تسهیل کاربرد مشترک محتوای فرایند دو استاندارد فرایند چرخه عمر در نظر گرفته شده است. استاندارد ISO/IEC/TR 24748 راهنمای تکی و محکم در مورد مدیریت چرخه عمر سامانه‌ها و نرم‌افزار ارائه می‌کند. هدف آن، کمک به حصول اطمینان از این است که سازگاری در مفاهیم سامانه و مفاهیم چرخه عمر، مدل‌ها، مراحل، فرایندها، کاربرد فرایند، تکرار و بازگشت فرایندها طی چرخه عمر، نقطه دیدگاه‌های مهم، تطبیق و استفاده در دامنه‌های متنوع است. استاندارد ISO/IEC 24748-1 استفاده از مدل چرخه عمر برای سامانه‌ها در زمینه استاندارد ISO/IEC 15288 ترسیم می‌کند و ترسیم مربوط به استفاده از مدل چرخه عمر برای نرم‌افزار را در زمینه استاندارد ISO/IEC 12207 ارائه می‌کند.

قسمت چهارم این مجموعه استاندارد، به کاربر آزادی انتخاب می‌دهد چه آنها از فرآورده‌های خاصی که «مورد تضمین» نامیده می‌شود، استفاده کنند یا از مستندات اطلاعات مرتبط با تضمین در دیگر مستندات استفاده کنند. هدف دست‌یابی به ادعای سطح بالا و نشان دادن دست‌یابی به اطلاعات ادعا برای مقدار بحرانی خاصیت برای یک ذی‌نفع مرتبط است. فرایندهای چرخه عمر، فعالیت‌ها و وظایف، نیاز به بازتاب هردوی محقق کردن سامانه کافی و مطمئن بودن از این که سامانه به قدرکافی به اطمینان موردنیاز سودبران دست می‌یابد را دارد.

کاربران قسمت چهارم این مجموعه استاندارد، ممکن است نیاز به ارزشیابی مخاطره و مدیریت مخاطره، سنجش و فرایندهای نیازمندی‌هایی که کامل‌تر از برطرف‌سازی‌های ارائه شده در استاندارد ISO/IEC 15288 و ISO/IEC 12207 ساخته شدند، باشند. سه استاندارد بین‌المللی، ISO/IEC 16085، *مدیریت مخاطره*، ISO/IEC 15939، *سنجش* و ISO/IEC/IEEE 29148، *مهندسی نیازمندی‌ها*، به منظور استفاده با استانداردهای ISO/IEC 15288 و ISO/IEC 12207 در ارائه جزییات بیشتر برای این سه فرایند طراحی شده است. دیگر استانداردهایی که نیازمندی‌های مفید و راهنمایی برای فرایندهای انتخاب شده ارائه می‌کنند، استانداردهای ISO/IEC /IEEE 15289 برای مستندسازی نتایج برگرفته از اجرای فرایندهای چرخه عمر و ISO/IEC/IEEE 16326 برای فرایند مدیریت پروژه است.

استاندارد ISO/IEC 15026 به منظور مطابقت با این استانداردهای فرایند چرخه عمر در نظر گرفته می‌شود. هدف کلی تضمین، انتخاب ادعاهایی است که باید از آن اطمینان حاصل شود، طرح‌ریزی مرتبط با تضمین و ساختن و نگهداشت مورد تضمین دارای تأثیراتی داخل فرایندهای چرخه عمر است.

۲-۹ فعالیت‌های تضمین در چرخه عمر

اجرای مجموعه فعالیت‌های تضمین طرح‌ریزی شده و نظام‌مند، نیاز به ارائه موجبات اطمینان در خواص سامانه شود. این فعالیت‌ها به منظور حصول اطمینان از این که هردو فرایندها و سامانه‌ها منطبق با نیازمندی‌های آن‌ها، استانداردها و راهنما و رویه‌های تعریف شده است، طراحی می‌شود [۱۴۵]. «فرایندها» در این زمینه شامل تمامی فعالیت‌های مشمول در طراحی، توسعه و نگاهداری سامانه است. برای نرم‌افزار «محصولات نرم‌افزار» شامل خود نرم‌افزار، داده‌های مرتبط با آن، مستندسازی آن و پشتیبانی و گزارش‌دهی کار کاغذی تولید شده به عنوان قسمتی از فرایند نرم‌افزار (به طور مثال، نتایج آزمون و استدلال‌های تضمین) و همچنین هرچیز دیگری که به منظور تکمیل مورد تضمین ضروری است. «نیازمندی‌ها» شامل نیازمندی‌هایی برای خواصی است که توصیه می‌شود نشان داده شوند و غایت مبتنی بر نیازمندی‌هایی به منظور محدودسازی، کاهش یا مدیریت هزین‌های مرتبط با خاصیت و خسران باشد. «استانداردها و راهنما» ممکن است فنی و تعریف کننده فناوری‌هایی باشد که می‌تواند در سامانه یا نرم‌افزار به کار رود یا ممکن است غیرفنی باشد و تعریف کننده جنبه‌های فرایندی باشد که پیش‌تر توسط «رویه‌هایی» که نیازمندی‌های ممکن سامانه برآورده شود.

مدیریت فعالیت‌های چرخه عمر شامل سامان‌دهی هردو فعالیت به طور مستقیم با مشمول کردن اطلاعات مرتبط با تضمین و اثری که اطلاعات مرتبط با تضمین بر روی فعالیت‌های دیگر دارد. این مدیریت بهترین انجامی است که ادعاهای سطح بالا ار ابتدای توسعه مفهوم متوجه آن هستند که به منظور تحت تأثیر قرار دادن تمامی فعالیت‌ها و سامانه‌ها به کار می‌رود [۱۴۰] و پیوست ب در [۲۲] و قسمت جدایی‌ناپذیری از فرایند مهندسی کلی در می‌آید. این فعالیت‌ها می‌تواند تنها اگر سامانه و مجموعه اطلاعات نشان دهنده دست‌یابی به آن دسته ادعاهایی است که به طور هم‌زمان توسعه داده شده است.

این امر، ماهیت موازی از منطق توسعه و استدلال است ولی یکی از سودهای توسعه هم‌زمانی توسعه سامانه و مورد تضمین خود است. فرایند توسعه و سامانه می‌تواند نه تنها در دست‌یابی به ادعا کمک کند بلکه به روشی انجام شود که بتواند نشان دهد که توسط مورد تضمین به قدر کفایت است. مورد تضمین با وادارا کردن سامانه به توسعه به روشی که استدلال عملی‌تر از ساختن باشد، آن را تحت تأثیر می‌دهد. این امر اغلب منجر به سامانه ساده‌تری (به طور کمینه داخلی) می‌شود، سامانه‌ای که عناصر سامانه می‌تواند به تنهایی به منظور نشان دادن زیرادعاهای قطعی به کار می‌رود و ترتیبی از عناصر سامانه از قبیل برهان در مورد ترکیب، هردو داخل حالت صنعتی و عملی است. فرایندهای هم‌زمان می‌تواند شامل نیازمندی‌های پوشش دهنده شرایط و رویدادهای بیشتر و همچنین روش‌ها، قابلیت ارجاع شایسته به کار می‌روند که توقف‌هایی تولید می‌کند و اعتبارسنجی و تصدیق هدف انچه نیاز به نشان داده شدن و نشان دادن کفایت است می‌شود.

۱۰ خلاصه

این استاندارد به منظور ارائه درک کافی به کاربران تمامی قسمت‌های این مجموعه استاندارد از مفاهیم و مجموعه اصطلاحات به کاررفته در این مجموعه استاندارد که قبلاً ممکن است میان جوامع به خدمت گرفته شده به اشتراک گذاشته نشده، نوشته شده است. توصیه می‌شود توضیح از آنچه در هر قسمت از این مجموعه استاندارد پوشش داده می‌شود، مبنایی برای انتخاب و به کارگیری آن قسمت‌ها و همچنین منطق پشت سازمان‌دهی این مجموعه استاندارد از خود استانداردها ارائه کند.

کتاب‌نامه

[1] AbranA., & MooreJ.W. (Executive editors); Pierre Bourque, Robert Dupuis, Leonard Tripp (Editors). Guide to the Software Engineering Body of Knowledge. 2004 Edition. Los Alamitos, California: IEEE Computer Society, Feb. 16, 2004. Available at http://www.swebok.org

[2] AdamskiA., & WestrumR. Requisite imagination: The fine art of anticipating what might go wrong." In: [55], p. 193-220, 2003

[3] Adelard. The Adelard Safety Case Development Manual. Available at http://www.adelard.com/web/hnav/resources/ascad

[4] AlexanderI Systems Engineering Isn't Just Software. 2001. Available at http://easyweb.easynet.co.uk/~iany/consultancy/systems_engineering/se_isnt_just_sw.htm.

[5] AllenJ.H., BarumS., EllisonR.J., McGrawG., MeadN.R. Software Security Engineering: A Guide for Project Managers. Addison-Wesley, 2008

[6] AltmanW., AnkrumT., BrachW. Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants: A Report to Congress. U.S. Nuclear Regulatory Commission:Office of Inspection and Enforcement, 1987

[7] AndersonJ.P. Computer Security Technology Planning Study Volume I, ESDTR-73-51, Vol. I, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730, Oct. 1972.

[8] AndersonR.J. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley and Sons, Second Edition, 2008

[9] AnkrumT.S., & KromholzA.H. Structured Assurance Cases: Three Common Standards," Ninth IEEE International Symposium on High-Assurance Systems Engineering (HASE'05), pp. 99-108, 2005

[10] ArmstrongJ.M., & PaynterS.P. The Deconstruction of Safety Arguments through Adversarial Counter-argument. School of Computing Science, Newcastle University CS-TR-832, 2004

[11] AtchisonB., LindsayP., TombsD. A Case Study in Software Safety Assurance Using Formal Methods. Technical Report No. 99-31. Sept. 1999

[12] ATSIN Number 17 Issued 9. Lapses and Mistakes. Air Traffic Services Information Notice, Safety Regulation Group, ATS Standards Department. UK Civil Aviation Authority, August 2002

[13] BahillA.T., & GissingB. Re-evaluating Systems Engineering Concepts Using Systems Thinking. IEEE Trans. Syst. Man Cybern. C. 1998 November, 28 (4) pp. 516–527

[14] BergC.J. High-Assurance Design: Architecting Secure and Reliable Enterprise Applications. Addison Wesley, 2006

[15] BernsteinLawrence, & YuhasC. M. Trustworthy Systems through Quantitative Software Engineering. Wiley-IEEE Computer Society Press, 2005. About reliability not security

[16] BishopM., & EngleS. The Software Assurance CBK and University Curricula. Proceedings of the 10th Colloquium for Information Systems Security Education, 2006

[17] BishopM. Computer Security: Art and Practice. Addison-Wesley, 2003

[18] BishopP., & BloomfieldR. A Methodology for Safety Case Development. Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham. 1998

[19] BishopP., & BloomfieldR. The SHIP Safety Case Approach. SafeComp95, Belgirate, Italy. Oct 1995

[20] BuehnerM.J., & ChengP.W. Causal Learning. In: The Cambridge Handbook of Thinking and Reasoning, (MorrisonR., & HolyoakK.J. eds.). Cambridge University Press, 2005, pp. 143–68.

[21] CannonJ.C. Privacy. Addison Wesley, 2005

[22] CAP 670 Air Traffic Services Safety Requirements. UK Civil Aviation Authority Safety Regulation Group, 2012

[23] CAP 730 Safety Management Systems for Air Traffic Management A Guide to Implementation. UK Civil Aviation Authority Safety Regulation Group, 12 September 2002

[24] CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers, 10 December 2010

[25] ChungL. et al. Non-Functional Requirements in Software Engineering. Kluwer, 1999

[26] ClarkD.D., & WilsonD.R. A Comparison of Commercial and Military Computer Security Policies, Proc. of the 1987 IEEE Symposium on Security and Privacy, IEEE, pp. 184-196, 1987

[27] CNSS. National Information Assurance Glossary, CNSS Instruction No. 4009, 26 April 2010. Available at http://www.cnss.gov/full-index.html

[28] Committee onInformationSystemsTrustworthiness. Trust in Cyberspace, Computer Science and Telecommunications Board. National Research Council, 1999

[29] Committee on National Security Systems (CNSS) Instruction 4009: National Information Assurance (IA) Glossary. Revised May 2003. Available at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[30] CommonCriteriaRecognitionArrangement(CCRA). Common Criteria v3.1 Revision 2. NIAP September 2007. Available at http://www.commoncriteriaportal.org.

[31] CommonWeaknessesEnumeration. MITRE, 2012. Available at http://cwe.mitre.org

[32] CookeN.J., GormanJ.C., WinnerJ.L. Team Cogitation. p. 239-268 In: [43]

[33] CourtoisP.-J. Justifying the Dependability of Computer-based Systems: With Applications in Nuclear Engineering. Springer, 2008

[34] CranorL., & GarfinkelS. Security and Usability: Designing Secure Systems that People Can Use. O'Reilly, 2005

[35] Dayton-Johnson. Jeff. Natural disasters and adaptive capacity. OECD Development Centre Research programme on: Market Access, Capacity Building and Competitiveness. Working Paper No. 237 DEV/DOC(2004)06, August 2004

[36] Department of Defense Directive 8500.1 (6 February 2003). Information Assurance (IA), Washington, DC: US Department of Defense, ASD(NII)/DoD CIO, April 23, 2007. Available at http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.

[37] Department of Defense Strategic Defense Initiative Organization. Trusted Software Development Methodology, SDI-S-SD-91-000007, vol. 1, 17 June 1992

[38] Department of Homeland Security National Cyber Security Division's "Build Security In" (BSI) web site, 2012, http://buildsecurityin.us-cert.gov

[39] DependabilityResearchGroup. Safety Cases. University of Virginia, Available at: http://dependability.cs.virginia.edu/info/Safety_Cases

[40] DespotouG., & KellyT. Extending the Safety Case Concept to Address Dependability, Proceedings of the 22nd International System Safety Conference, 2004

[41] DowdM., McDonaldJ., SchuhJ. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison-Wesley, 2006

[42] DunbarK., & FugelsangJ. Scientific Thinking and Reasoning. In: [59], p. 705–727

[43] DursoF.T., NickersonR.S., DumaisS.T., LewandowskyS., PerfectT.J. eds. Handbook of Applied Cognition2nd edition . Wiley, 2007

[44] EllsworthP.C. Legal Reasoning. In: [59], p. 685–704

[45] EricssonK.A., CharnessN., FeltovichP.J., HoffmanR.R. eds. The Cambridge Handbook of Expertise and Expert Performance. Cambridge University Press, 2006

[46] FentonN., LittlewoodB., NeilM., StriginiL., SutcliffeA., WrightD. Assessing dependability of safety critical systems using diverse evidence. IEE Proc. Softw.1998 145 (1) pp. 35–39

[47] GasserM. Building a Secure Computer System. Van Nostrand Reinhold, 1988. Available at http://deke.ruc.edu.cn/wshi/readings/cs02.pdf

[48] GrayJ.W. Probabilistic Interference. Proceedings of the IEEE Symposium on Research in Security and Privacy. IEEE, p. 170-179, 1990

[49] GreenwellW., StrunkE., KnightJ. Failure Analysis and the Safety-Case Lifecycle. IFIP Working Conference on Human Error, Safety and System Development (HESSD) Toulouse, France. Aug 2004

[50] GreenwellW.S., KnightJ.C., PeaseJ.J. A Taxonomy of Fallacies in System Safety Arguments. 24th International System Safety Conference, Albuquerque, NM, August 2006

[51] HallA., & ChapmanR. Correctness by Construction: Developing a Commercial Secure System. IEEE Softw.2002 Jan/Feb, 19 (1) pp. 18–25

[52] HerrmannD.S. Software Safety and Reliability. IEEE Computer Society Press, 1999

[53] HoglundG., & McGrawG. Exploiting Software: How to break code. Addison-Wesley, 2004

[54] HollnagelE., WoodsD.D., LevesonN. eds. Resilience Engineering: Concepts and Precepts. Ashgate Pub Co, 2006

[55] HollnagelE. ed. Handbook of cognitive task design. Lawrence Erlbaum Associates, 2003

[56] HollnagelE. Human Error: Trick or Treat?. In: [43], p. 219–238

[57] HollnagelE. Barriers and Accident Prevention. Ashgate, 2004

[58] HollnagelE. Human Factors: From Liability to Asset. Presentation, 2007. Available at www.vtt.fi/liitetiedostot/muut/Hollnagel.pdf

[59] HolyoakK.J., & MorrisonR.G. eds. The Cambridge Handbook of Thinking and Reasoning. Cambridge University Press, 2005

[60] HowardM., & LeBlancD.C. Writing Secure Code. Microsoft Press, Second Edition, 2002

[61] HowardM., & LipnerS. The Security Development Lifecycle. Microsoft Press, 2006

[62] HowellC. Assurance Cases for Security Workshop (follow-on workshop of the 2004 Symposium on Dependable Systems and Networks), June, 2005

[63] IEC 60050-191, International Electrotechnical Vocabulary, Chapter 191: Dependability and Quality of Service

[64] IEC 60300Dependability management [several parts]

[65] IEC 60300-3-15 ed1.0 (2009-06) De

[66] [66] IEC 60300-3-2 ed.2.0 (2004-11), Dependability management – Part 3-2: Application guide - Collection of dependability data from the field

[67] IEC 60812 ed2.0 (2006-01), Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)

[68] IEC 61025 ed2.0 (2006-12), Fault tree analysis (FTA)

[69] IEC 61078 ed2.0 (2006-01), Analysis techniques for dependability - Reliability block diagram and Boolean methods

[70] IEC 61508 ed2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems[several parts]

[71] IEC 61508-7 ed2.0 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures

[72] IEC 61511 ed1.0, Functional safety - Safety instrumented systems for the process industry sector[several parts]

[73] IEC 61882 ed1.0 (2001-05), Hazard and operability studies (HAZOP studies) - Application guide

[74] IEC CD 62741 ed.1.0, Reliability of systems, equipment, and components. Guide to the demonstration of dependability requirements. The dependability case

[75] StdIEEE 1228-1994, IEEE Standard for Software Safety Plans

[76] InternationalCouncil onSystemsEngineeringINCOSE. Guide to Systems Engineering Body of Knowledge (G2SEBoK). Available at http://g2sebok.incose.org/

[77] ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction

[78] ISO 13849, Safety of machinery — Safety-related parts of control systems[three parts]

[79] ISO 14620, Space systems — Safety requirements[three parts]

[80] ISO 14625:2007, Space systems — Ground support equipment for use at launch, landing or retrieval sites — General requirements

[81] ISO 19706:2011, Guidelines for assessing the fire threat to people

[82] ISO 20282, Ease of operation of everyday products [four parts]

[83] ISO 2394:1998, General principles on reliability for structures

[84] ISO 28003:2007, Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems

[85] ISO 9241-400:2007, Ergonomics of human — system interaction — Part 400: Principles and requirements for physical input devices

[86] ISO/IEC 12207:2008, Systems and software engineering — Software life cycle processes

[87] ISO/IEC 15288:2008, Systems and software engineering — System life cycle processes

[88] ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security[three parts]

[89] ISO/IEC TR 15443, Information technology — Security techniques — Security assurance framework[two parts]

[90] ISO/IEC 15939:2007, Systems and software engineering — Measurement process

[91] ISO/IEC 16085:2006, Systems and software engineering — Life cycle processes — Risk Management

[92] ISO/IEC/IEEE 16326:2009, Systems and software engineering — Life cycle management - Project management

[93] ISO/IEC 18014, Information technology — Security techniques — Time-stamping services [three parts]

[94] ISO/IEC 18028, Information technology — Security techniques — IT network security [many parts]

[95] ISO/IEC 19770, Information technology — Software Asset Management[two parts]

[96] ISO/IEC 21827:2008, Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

[97] ISO/IEC 2382-14:1997, Information technology — Vocabulary — Part 14: Reliability, maintainability and availability

[98] ISO/IEC 25000:2005, Software Engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE

[99] ISO/IEC 25010:2011, Systems and software engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — System and software quality models

[100] ISO/IEC 25012:2008, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model

[101] ISO/IEC 25020:2007, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Measurement reference model and guide

[102] ISO/IEC 25030:2007, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Quality requirements

[103] ISO/IEC 25040:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process

[104] ISO/IEC 25051:2006, Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing

[105] ISO/IEC 26702:2007, Systems engineering — Application and management of the systems engineering process

[106] ISO/IEC 27000:2012, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[107] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems – Requirements

[108] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls

[109] ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement

[110] ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management

[111] ISO/IEC 27006:2011, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[112] ISO/IEC 27011:2008, Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

[113] ISO/IEC/IEEE 42010:2011, Systems and software engineering — Architecture Description

[114] ISO/IEC 90003:2004, Software engineering — Guidelines for the application of ISO 9001:2000 to computer software

[115] ISO/IEC TR 15446:2009, Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

[116] ISO/IEC TR 19791:2010, Information technology — Security techniques — Security assessment of operational systems

[117] ISO/IEC TR 24748-1:2010, Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management

[118] ISO/TR 16982:2002, Ergonomics of human-system interaction — Usability methods supporting human-centred design

[119] ISO/TR 18529:2000, Ergonomics — Ergonomics of human-system interaction — Human-centred lifecycle process descriptions

[120] ISO/TR 27809:2007, Health informatics — Measures for ensuring patient safety of health software

[121] ISO/TS 25238:2007, Health informatics — Classification of safety risks from health software

[122] KazmanR., AsundiJ., KleinM. Making Architecture Design Decisions: An Economic Approach, SEI-2002-TR-035. Software Engineering Institute, Carnegie Mellon University, 2002

[123] KazmanR., KleinM., ClementsP. ATAM: Method for Architecture Evaluating the Quality Attributes of a Software Architecture. Technical Report CMU/SEI-200-TR004. Software Engineering Institute, Carnegie Mellon University, 2000

[124] KellyT. Arguing Safety – A Systematic Approach to Managing Safety Cases. Doctorial Thesis – University of York: Department of Computer Science. Sept 1998

[125] KellyT. Reviewing Assurance Arguments - A Step-by-Step Approach. Workshop on Assurance Cases for Security: The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[126] KellyT., & WeaverR. The Goal Structuring Notation – A Safety Argument Notation. Workshop on Assurance Cases: Best Practices, Possible Obstacles, and Future Opportunities, Florence, Italy. July 2004

[127] LadkinP. The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed. 29 Aug 2002. Available at http://www.rvs.uni bielefeld.de/publications/Reports/SCflawed-paper.html

[128] LandwehrC. Computer Security. IJIS. 2001, 1pp. 3–13

[129] LautieriS., CooperD., JacksonD. SafSec: Commonalities Between Safety and Security Assurance. Proceedings of the Thirteenth Safety Critical Systems Symposium - Southampton, 2005

[130] LeBoeufR.A., & ShafirE.B. Decision Making. In: [59], p. 243–266

[131] LevesonN. A Systems-Theoretic Approach to Safety in Software-Intensive Systems, IEEE Trans.Dependable Sec. Comput. 2004, 1 (1) pp. 66-86

[132] LipnerS., & HowardM. The Trustworthy Computing Security Development Lifecycle, Microsoft, 2005. Available at http://msdn.microsoft.com/en-us/library/ms995349.aspx

[133] MaguireR. Safety Cases abd Safety Reports: Meaning, Motivation and Management. Ashgate, 2006

[134] McDermidJ. Software Safety: Where's the Evidence?6th Australian Workshop on Industrial Experience with Safety Critical Systems and Software (SCS '01), Brisbane. 2001

[135] McGrawG. Software Security: Building Security In. Addison Wesley, 2006

[136] McLeanJ. Security Models. In: Encyclopedia of Software Engineering, (MarciniakJ. ed.). Wiley, 1994

[137] MeierJ.D., MackmanA., VasireddyS., DunnerM., EscamillaR., MurukanA. Improving Web Application Security: Threats and Countermeasures, Microsoft, 2004. Available at: http://download.microsoft.com/download/d/8/c/d8c02f31-64af-438c-a9f4-e31acb8e3333/Threats_Countermeasures.pdf

[138] MerkowM.S., & BreithauptJ. Computer Security Assurance Using the Common Criteria. Thompson Delamr Learning, 2005

[139] Ministry of Defence. Defence Standard 00-42 Issue 2, Reliability and Maintainability (R&M) Assurance Guidance. Part 3, R&M Case, 6 June 2003

[140] Ministry Of Defence. Defence Standard 00-55 (PART 1)/Issue 2, Requirements for Safety Related Software in Defence Equipment Part 1: Requirements, 21 August 1997

[141] Ministry of Defence. Defence Standard 00-55 (PART 2)/Issue 2, Requirements for Safety Related Software in Defence Equipment Part 2: Guidance, 21 August 1997

[142] Ministry of Defence. Interim Defence Standard 00-56, Safety Management Requirements for Defence Systems Part 1: Requirements, 17 December 2004

[143] Ministry of Defence. Interim Defence Standard 00-56, Safety Management Requirements for Defence Systems Part 2: Guidance on Establishing a Means of Complying with Part 1, 17 December 2004

[144] MooreA., KlinkerE., MihelcicD. How to Construct Formal Arguments that Persuade Certifiers. In: Industrial Strength Formal Methods in Practice. Academic Press. 1999

[145] NationalAeronautics andSpaceAdministration(NASA) SoftwareAssuranceGuidebook. September 1989 (NASA-GB-A201). Available at http://www.hq.nasa.gov/office/codeq/doctree/nasa_gb_a201.pdf

[146] NationalOffshorePetroleumSafetyAuthority. Safety case. [Online Documents [cited on: 20 Jun 2012] Available at http://www.nopsema.gov.au/safety/safety-case/

[147] NationalResearchCouncil(NRC) ComputerScience andTelecommunicationsBoard. (CSTB). Cybersecurity Today and Tomorrow: Pay Now or Pay Later. National Academies Press, 2002. Available at http://www.nap.edu/topics.php?topic=320&start=10

[148] National Security Agency, The Information Systems Security Engineering Process (IATF) v3.1. 2002

[149] NavalResearchLaboratory. Handbook for the Computer Security Certification of Trusted Systems. US Naval Research Laboratory, 1995

[150] NDIA SystemAssuranceCommittee. Engineering for System Assurance. National Defense Industrial Association, USA, 2008

[151] NIST. Federal Information Processing Standards Publication (FIPS PUB) 200: Minimum Security Requirements for Federal Information and Information Systems. March 2006. Available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[152] NIST. NIST Special Publication 800-27, Rev A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Revision A, June 2004. Available at http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[153] NIST. NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security, December 2001. Available at http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[154] Process Framework O.P.E.N. Safety Cases. [Online Document cited on: 20 Jun 2012] Available at: http://www.opfro.org/index.html?Components/WorkProducts/SafetySet/SafetySet.html~Contents

[155] OPSI. The Offshore Installations (Safety Case) Regulations 2005. [Online Document cited on: 20 June 2012.] Available at http://www.opsi.gov.uk/si/si2005/20053117.htm

[156] ParkJ., MontroseB., FroscherJ. Tools for Information Security Assurance Arguments. DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, 2001

[157] PetroskiH. Design Paradigms. Cambridge University Press, 1994

[158] PrasadD. Dependable Systems Integration using Measurement Theory and Decision Analysis, PhD Thesis, Department of Computer Science, University of York, UK, 1998

[159] PSM Safety & Security TWG. Security Measurement. Nov 2004

[160] PullumL.L. Software Fault Tolerance. Artech House, 2001

[161] RandellB., & KoutnyM. Failures: Their Definition, Modelling and Analysis. School of Computing Science, Newcastle University CS-TR NO 994, Dec 2006RandellB., & RushbyJ.M. Distributed Secure Systems: Then and Now. CS-TR No 1052 School of Computing Science, Newcastle University, Oct 2007

[162] RechtinE. Systems Architecting of Organizations: Why Eagles Can't Swim. CRC Press, Boca Raton, FL, 2000

[163] RedwineS.T. Jr. ed. Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software Version 1.1. US Department of Homeland Security, September 2006

[164] RedwineS.T. Jr. The Quality of Assurance Cases. Workshop on Assurance Cases for Security: The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[165] RedwineS.T. Jr., & DavisN. eds. Processes for Producing Secure Software: Towards Secure Software. Vols. I and II. Washington, D.C.: National Cyber Security Partnership, 2004. Available at http://www.cigital.com/papers/download/secure_software_process.pdf

[166] RossK.G., ShaferJ.L., KleinG. Professional Judgements and 'Naturalistic Decision Making'. In: [45], p. 403-420

[167] RossR. et al. Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, Aug 2009. Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[168] SAE JA1000, Reliability Program Standard, SAE International, June 1998. Available at http://www.sae.org

[169] SaltzerJ.H., & SchroederM.D. The protection of information in computer systems. Proc. IEEE. 1975, 63 (9) pp. 1278–1308. Available at: http://cap-lore.com/CapTheory/ProtInf/

[170] Seminal Papers - History of Computer Security Project, University of California Davis Computer Security Laboratory. Available at: http://seclab.cs.ucdavis.edu/projects/history/seminal.html

[171] Serene. "Safety argument." [Online Document] [cited on: 13 Feb 2007] Available at: http://www2.dcs.qmul.ac.uk/~norman/SERENE_Help/sereneSafety_argument.htm

[172] SeversonK. Yucca Mountain Safety Case Focus of NWTRB September Meeting. United States Nuclear Waste Technical Review Board. Aug 2006

[173] SieckW.R., & KleinG. Decision making. In: [43], p. 195-218

[174] Software and Systems Engineering Vocabulary (sevocab). Available at www.computer.org/sevocab

[175] SommervilleI. Software Engineering. Pearson Education, Eighth Edition, 2006

[176] StoneburnerG., HaydenC., FeringaA. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, NIST Special Publication 800-27 Rev A, June 2004

[177] StoreyN. Safety-Critical Computer Systems. Addison Wesley, 1996

[178] StrunkE., & KnightJ. The Essential Synthesis of Problem Frames and Assurance Cases. IWAAPF'06, Shanghai, China. May 2006

[179] SwiderskiF., & SnyderW. Threat Modeling. Microsoft Press, 2004

[180] U.S. NRC. "Quality Assurance Case Studies at Construction Projects."

[181] VanfleetW.M. et al. MILS: Architecture for High Assurance Embedded Computing," Crosstalk, August, 2005

[182] ViegaJ., & McGrawG. Building Secure Software: How to Avoid Security Problems the Right Way. Addison Wesley, Reading, MA, 2001

[183] WalkerV.R. Risk Regulation and the 'Faces' of Uncertainty, Risk: Health, Safety and Environment. p. 27-38, Winter 1998

[184] WareW.H. Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security, The RAND Corporation, Santa Monica, CA (Feb. 1970)

[185] WeaverR. The Safety of Software – Constructing and Assuring Arguments. Doctorial Thesis – University of York: Department of Computer Science. 2003

[186] WeaverR., FennJ., KellyT. A Pragmatic Approach to Reasoning about the Assurance of Safety Arguments. 8th Australian Workshop on Safety Critical Systems and Software (SCS'03), Canberra. 2003

[187] WhittakerJ.A., & ThompsonH.H. How to Break Software Security: Effective Techniques for Security Testing. Pearson Education, 2004

[188] WilliamsJ., & SchaeferM. Pretty Good Assurance. Proceedings of the New Security Paradigms Workshop. IEEE Computer Society Press. 1995

[189] WilliamsJ.R., & JelenG.F. A Framework for Reasoning about Assurance, Document Number ATR 97043, Arca Systems, Inc., 23 April 1998

[190] YatesJ.F., & TschirhartM.D. Decision-Making Expertise. In: [45], p. 421-438

[191] YeeK.-P . User interaction design for secure systems. Proceedings of the 4th Internatio